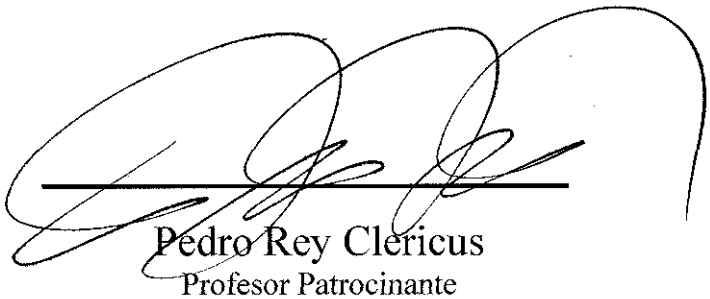
Universidad Austral de Chile
Facultad de Ciencias de la Ingeniería
Escuela de Ingeniería Civil Electrónica

HOMOLOGACIÓN DE UN SERVIDOR DE VOZ SOBRE IP CON SOPORTE IPV4 E IPV6 EN UN ROUTER INALÁMBRICO

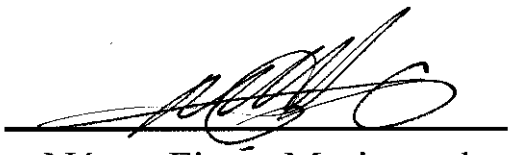
Trabajo para optar al título de:
Ingeniero en Electrónica.

Profesor Patrocinante:
Sr. Pedro Rey Clericus.
Ingeniero Electrónico,
Licenciado en Ciencias de la Ingeniería,
Diplomado en Ciencias de la Ingeniería.

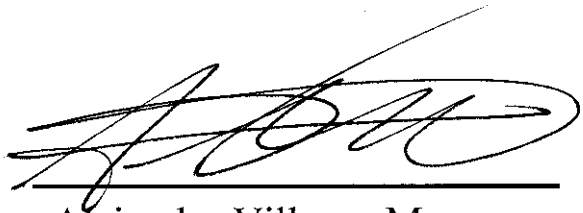
RAUL PAUL CAULIER CISTERNA
VALDIVIA - CHILE
2008



Pedro Rey Clericus
Profesor Patrocinante



Néstor Fierro Morineaud
Profesor Informante



Alejandro Villegas Macaya
Profesor Informante

FECHA EXAMEN: 7 ABRIL 2008

"Hay que tener perseverancia y sobre todo confianza en ti mismo. Hay que creer que se está dotado para alguna cosa y que esta cosa hay que obtenerla cueste lo que cueste".

Marie Curie

Agradecimientos:

Siempre e creído que lo mas difícil de escribir y expresar es lo que sale del corazón, es por esto que puedo dar testimonio que lo mas difícil de escribir en esta tesis fueron estas palabra que aunque uno trate de poner a todas las personas importantes en mí vida, siempre van a faltar, ya que el espacio no es mucho y los sentimientos son artos.

Comenzare agradeciendo a mis amigos, grandes personas que me enseñaron a caviar mi visión del mundo y darme cuenta que la vida estaba llena de momentos felices y que los momentos tristes, al compartirlos con personas especiales, se asían mucho mas llevaderos y soportables. Le agradezco a esas personas que estuvieron conmigo cuando el mundo ya no le quedan palabras y un gesto, una palabra o un abrazo dicen tanto que no puedes contener las lagrimas y decir gracias o un te quiero; a esas personas les doy gracias ya que si no hubiesen estado en mi vida, quizás yo nunca hubiese terminado la universidad ni menos este trabajo de titilación. Cada una de ellas me entrego algo especial, como mi gran amigo Cristian Paredes, persona que me dio alegría y me enseño que para estar bien con el mundo hay que recibirlo con una sonrisa y que el mundo tiene un sentido mas grande de lo que uno puede ver. También es importante destacar a tres personajes que estuvieron acompañándome siempre, alegrando las tardes de responsabilidades y de estudios, ha esas tres personas especiales, que abrieron su corazón para recibirme como uno de ellos y que me enseñaron que la vida puede ser mas bella de lo que yo pensaba, que al ver las cosas desde varias perspectivas uno se podía dar cuenta que el mundo estaba lleno de miles de bellezas que el hombre común las rechaza por miedo a lo que puedan pensar, esas tres almas libres que me hacen reír cuando yo quiero llorar, que me apoyan cuando me siento desolado, que me alegran y puedo compartir, cuando nadie quiere estar, esas personas son Cesar Sandoval, Félix Nahuelpan y Daniel Vidal, que cada vez que los veo me hacen sentir que la vida es ahora y hay que aprovecharla por que algún día puede cambiar. También agradece a una persona que con su sentido tan particular de ver la vida me ayudo a darme cuenta que a veces, aunque creas que no puedes salir de donde estas, si lo vez de otra forma igual puedes salir de ahí, esa persona es Rodolfo Miralles, que por diversos motivos quizás no es posible compartir como me gustaría con él, pero igual lo considero una persona sumamente importante en mi vida y me atrevo a decirle amigo con toda y cada una de sus letras, por que es así como me hace sentir a pesar de todas las cosas que hemos pasado juntos.

Ahora continuare con dos personar que no pueden faltar; quizás entre ellas no exista una gran afinidad, pero si a mí me han hecho sentir la persona mas maravillosa del mundo, esas personas son la Tía Edith Palma y la Elena Alvarado. La tía Edith, una persona que pueden decir mucho de ella, pero conmigo a sido correctiva y aconsejadora, me ha hecho reflexionar en muchas cosas en esta vida y me ha dado una compañía en un lugar que quizás no todos tiene la suerte de tenerla, ha diferencia quizás de algunos amigos que están cercano a ella, no puedo decir que ha sido como una madre, pero si puedo decir que ha sido una angelito, que me a cuidado y apoyado en circunstancias que lo necesitaba, y me ha dado siempre ese consejo preciso que me ha llevado a tomar decisiones muy importantes en la vida y me ha llevado por el camino de la prudencia cunado mi padre no ha estado para ayudarme. La Elena, alma bella y pura que me dio la oportunidad de hacer lo que mas me gusta en la vida que es enseñar, ella me ayudo a iniciarme en lo que me gusta dándome la oportunidad de enseñar, sin ningún remuneración monetaria, pero lo que gane con ella es invaluable y no podría ponerle precio ya que ella sigue a mi lado y cada ves que esta conmigo me acoge y me hace sentir maravilloso aunque este lleno de defectos y muy querido por ella cosa que quizás ni siquiera me merezca, a ella le tengo que agradecer, que con su forma tan especial de ver la vida, la posibilidad de hoy tener a mi angelito de esmeralda a mi lado, y con sus consejos hacerme cada día mejor persona.

Unas personas que no puedo dejar de destacar por lo maravillosas y de gran corazón, son las Hermanas Misioneras Identes, que me han enseñado a ver al padre celestial de una forma que no lo conocía y me ayudaron a dejar entrar a Dios en mi corazón y ocupar esos espacios que lo único que tenia eran vicios, egoísmo, orgullo, rencor, dudas y soledad. Es por esto que a mis hermanitas Bernardita Moreno, Mónica Fuentes, Jessica Alarcón, Ana Maria Salinas y Fabiola Ojeda, les debo mi felicidad, ya que si no las hubiese conocido no seria tan feliz y no habría nunca conocido la felicidad de tener a Dios en mi corazón. Cada una de ellas con su carisma especial me regalaron una pequeña parte de ellas como la Jessica con esa forma tan fácil de alegrar los lugares en donde esta, la ana Maria con su forma de decir y enseñar tan en particular y bella que tiene, la Fabiola con su simpatía y espontaneidad que la caracteriza y la hace especial, la Mónica que con su preocupación hace que las personas se preocupe un poco mas de las cosas sencillas y de forma especial con la hermana y tía bernardita con su gran sabiduría y paciencia me ayudo a madurar y ser mejor persona, a no preocuparme por las tonteras y estupideces en que de repente me enrollaba, que mejor me preocupara de las cosas verdaderamente importantes y con su gran don que tiene, que la convierte en medio bruja para sus cosas, sabia exactamente que decirme y aconsejarme, de la forma exacta y precisa en el momento indicado. La extraño muchísimo a ella, pero se que en sus oraciones estoy presente y en cada instante se acuerda de mí como yo de ella, ya que fue una persona maravillosamente especial en mi vida y lo será hasta el final de ella. Es por esto que le agradezco a Dios cada instante de mi vida por darme la oportunidad de conocer a las personas mas bellas que tiene a su servicio a los hermanos y hermanas Indentes.

Continuare agradeciéndole ahora, a la persona que Dios me dio en mí vida, para que sea ella y solo ella la persona que le pueda entregar ese sentimiento tan bello y difícil de encontrar como es el amor, estas palabras son para mi angelito de esmeralda, es para Natalia Soto, mujer que conocí en circunstancias muy extrañas, pero de una forma muy celestial, es por eso que me atrevo a decir que Dios me la puso en mi camino para que este conmigo y me acompañe. Mi amorcito a sido esa personita que a llenado de luz mi vida, le dio un sentido y la levanto de donde estaba, me dio alegrías, penas, compañía y lo mas importante amor y felicidad a mi vida. Tengo que reconocer que si no hubiese aparecido ella en mi vida jamás podría haber terminado la universidad ni menos mi tesis ya que en los momentos en que no había nadie que me pueda ayudar, ella estuvo ahí para levantarme y caminar conmigo sin miedo y con total confianza en mi, es por esto que le agradezco a dios cada instante de mi vida por la mujer que puso a mi lado ya que sin ella no seria absolutamente nada y no seria tan feliz como lo soy ahora. También no puedo dejar de agradecerle a la familia de mi amorcito, ya que ellos me acogieron y me hacen sentir una persona especial entre ellos en especia quisiera destacar a don Rociel Soto Rogel, papá de mi polola ya que nunca había conocido una persona con tanta fuerza interior y con deseos de avanzar en la vida como él y lo mas importante, una persona que tiene honor y se puede confiar en él, cualidades que le ha transmitido a sus hijos y que en especial la Natalia, mi amorcito, lo ha sabido recibir y entender para tenerlo como uno de las grades enseñanzas y ejemplos que le ha dado su padre. Es por esto que le estoy tan agradecido y considere que tenia que estar en estas palabras ya que gracias a él existe esa personita maravillosa llamada Natalia soto y que además tengo el orgullo de decir que es mi polola y mas aun la mujer que amo.

Es importante también mencionar en estas líneas a mis profesores del instituto que siempre me han ayudado, y por sobre todo para el desarrollo de mi tesis. En especial a Roland Gloeckler, que fue mi profesor que me ayudo, guió y enseño todo para el desarrollo de mi tesis y cabe mencionar que sin él quizás nunca podría haber terminado mi tesis. También destacare a Don Pedro Rey que siempre me a aconsejado y me ha ayudado en todo lo que le he pedido, es por eso que estoy muy agradecido de el, por que sin su consejo, apoyo y comprensión, mi paso por la universidad hubiese sido demasiado tormentoso. También mencionaré a Don alejando Villegas, que fue mi profesor y ahora mi colega ya que con su preocupación y dedicación, me enseño a querer lo que ago y a preocuparme siempre de cada detalle de lo que estoy asiendo, así poder ser siempre un poco mejor que ayer.

Ahora, las personas quizás más importantes que un ser humano puede tener, la familia, que sin ella uno no es nada puesto que uno nace en una familia, vive con una familia y forma una familia. Agradecerle a mi tía Inés Frías por su apoyo y compañía incondicional en cada una de los momentos importantes de mi vida, mi tía cupe que siempre estuvo cuando la necesitaba, quizás nunca en presencia pero siempre sabia yo que su corazón me acompaña en cada uno de mis momentos importantes. Mi hermano Sebastián, que me enseña siempre con su forma de ser, la inocencia y la felicidad que un niño y ya joven debe tener, mi hermana Javiera que con su inocencia enternece mi corazón cada ves que la veo, y mi hermano danny un gran ejemplo para mi como también un apoyo incondicional en esas cosas simples y en los detalles que a tenido mí vida, además que sin él yo no me sentiría tan proseguido como me siento, ya que desde que era niño el siempre puso su mano para que yo no me cayera nunca. También parte de mi familia son la Marisol, mi segunda mamá, que la quiero muchísimo ya que ella me cuidaba y me quiso como su propio hijo y todavía se encuentra a mí lado ayudándome y asiéndome sentir especial; la cecilia con la javierita (vonchi) ya que esa niñita hermosa llena de alegría cada rincón de mi casa y curiosamente cada ves que he querido un abraso tierno e inocente siempre lo he tenido de ella siendo esos los momentos mas grandiosos que un hombre puede tener y por ultimo la Cote que es como mi otra hermana a la cual trato de proteger tanto como puedo ya que ella es como mi hermanita que me mira desde los cielos y me acompaña desde un rincón muy especial de mi corazón, que cada ves que la he necesitado ella esta y se refleja en mi cote, además que ella es muy bella y especial como persona.

Y por ultimo, las dos personas mas importantes que puedo tener mis papas, que han sido una guía y un gran apoyo en toda mi vida y ruego a Dios por que siempre sea así. Agradezco a mi Papá Raúl Caulier Segovía, que con su dureza pero con mucho amor me a criado de una forma muy correcta y llena de valores y esfuerzos, le agradezco ya que él nunca me a ocultado lo duro que es la vida y le debo a él la forma que tengo de superación ya que me la transmitió con sus enseñanzas y su rectitud, lo cual me permitió ser mejor persona en este mundo. Y mí Mamá Lucia Cisterna Mera, mujer grandiosa y santa, llena de virtudes y de amor asía sus hijos, la mejor medre que puede un hijo tener, me faltan palabras para describir lo que es ella ya que no se ha escrito palabra alguna ní se conoce siquiera la palabra exacta para describir lo grandiosa que es ella, es por esto que me cuesta tanto quizás agradecerle, pero lo que no me cuesta para nada es dejar expresado en estas palabras desde hoy y para siempre lo mucho que la AMO y la admiro ya que ella se merece esto y mucho mas, puesto que Dios no me pudo regalar mejor mujer que mi mamá para que me crié y me enseño con su corrección dulce y sincera y esa preocupación incondicional que solo ella me ha sabido dar toda su vida, por lo cual estoy agradecido y siempre viejita mía te amare.

Con esto ya finalizo mis agradecimiento, quizás hay mucha gente mas que me falta poner, y al leerlo encuentren faltas de ortografía y redacción, pero no quiero modificarle nada ahora, por que estas palabras salieron de los mas hondo de mi corazón y cada una de ellas esta escrita con un amor inmenso y no quisiera cambiar nada ya que estaría alterando algo puro y lleno de amor. Además aquí están los personajes mas importante en mi vida y por los cuales rezo cada noche a Dios para que les cuide y guié por un buen camino y quiero decir que me siento afortunado por tenerlos a mi lado ya que cada uno de ellos me ha entregado algo para mi vida que me ha hecho crecer como persona y como hombre para alcanzar esa perfección que busco que es la santidad.....Gracias Dios por los Angeles que me has enviado a mi vida.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El mundo de las comunicaciones avanza a pasos agigantados, ya que cada día aparece una nueva tecnología o forma de comunicaciones entre personas. El trabajo que se presenta a continuación trata de mejorar una de esta formas de comunicación, la VOIP que corresponde a la forma de comunicación a través de una red de datos TCP/IP, las cuales circundan el orbe y son de bastante utilización en estos días.

La idea fue mejorar un sistema, integrando los servicios presentes en un servidor de Voip en un router que permitiera la comunicación entre varios usuarios y teniendo como requisito fundamental la utilización de software libres, como los son el OPENWRT, que es un frimware basado en sistema de código abierto, como Linux, y el Openser, que corresponde a la versión de código abierto del famoso PBX para protocolo SIP, el SER (SIP EXPRESS ROUTER).

Además de contar con estar cualidades, el sistema responde a las dos versiones de IP existentes hoy en día en Internet, la IPv4 que es la que se utiliza tradicionalmente en las comunicaciones de RED y la IPv6 que es una versión mucho mas avanzada del protocolo IP existente, que mejorar los servicios de comunicación y aumentar la cantidad de usuarios que pueda soportar la red Internet, ya que se estaba quedando sin direcciones IP.

Lo más importante a destacar del trabajo, es que al momento de trabajar y escoger los equipos utilizados hay que ver las limitaciones de hardware que puedan tener, ya que éste es un factor muy importante a considerar al momento de trabajar con este tipo de programa, y más aun en un sistema tan reducido como lo es un router.

Todo esto fue desarrollado en el laboratorio de comunicaciones modernas del instituto de electricidad y electrónica con el fin de ser una herramienta útil para nuevos temas de investigación y desarrollo de esta singular tecnología.

ABSTRACT

The world of communications is advancing by leaps and bounds, because every day is a new technology or a new way to communicate to people. The work that follows attempts to improve one of this form of communication, VOIP corresponding to the form of communication through a data network TCP / IP, which encircle the globe and are quite use these days .

The idea was to improve a system, integrating services present in a server Voip in a router that would allow communication between multiple users and taking as a vital requirement using open-source software, such as are OPENWRT, which is a system based on frimware open source, such as Linux, and Openser, which corresponds to the open source version of the famous PBX to SIP protocol, the SER (SIP ROUTER EXPRESS).

In addition to being qualities, the system responds to the two versions of existing IP today on the Internet, IPv4 that is what is traditionally used in the communications network and IPv6 which is a much more advanced version of the IP protocol exist that improve communication facilities and increase the number of users that can withstand the Internet, as it was running out of IP addresses.

The most important highlight of the work is that when choosing to work and the equipment used to be see the limitations of hardware that may have, because this is a very important fact to consider when working with this type of program, and more even in a system as small as it is a router.

All of this was developed in the laboratory of the institute of modern communications electricity and electronics to be a useful tool for new research and development of this unique technology.

INTRODUCCIÓN

El siglo recién pasado, vio nacer una tecnología que su base fueron las redes de datos que servia para comunicar a persona dentro de áreas limitadas de usuarios, que no tenia ningún sentido y lo único que buscaba era compartir los recursos de una maquina que a veces no era la mas capas de satisfacer todas las necesidades que se le requerían. Todo esto dio pie al nacimiento de una nueva red mas amplia y que servia para enviar información a todas partes el mundo, gracias a la conexión de muchos ordenadores alrededor de orbe, la famosa RED INTERNET, que produjo un gran revuelo en las tecnologías de la información y que dio pie a un nuevo siglo, que no estaba basado en los conocimientos y en la capacidad que tenían las personas de dominar la información, transformándose en grandes mentes que tenían la verdad y la sabiduría para ellos, si no que se transformo en un mundo en donde el conocimiento y la verdad estaba a la disposición de todas las personas y que lo único que tenia que preocuparse era en donde buscar la información y el saber manejar esa información. Todo esto produjo un cambio en la actitud de las personas alcanzando un nuevo grado de evolución y permitiendo el rápido desarrollo de las tecnologías basadas en esta red, que se montaba sobre una pila de protocolos el cual el más importante correspondía al protocolo IP.

La tendencia de todas las tecnologías de la información es utilizar una sola red para los distintos tipos de servicios, como los son el teléfono, la televisión, los datos, y la red que puede satisfacer todos estos servicios es la red IP, que se encuentra a disposición de todas las personas, en sus distintos formatos, cableada e inalámbrica. En el futuro, se proyecta que esta red sea la llamada RED de REDES, solo quedando esta como la gran dominadora del mundo y que solo sobre ella estén montados los servicios básicos de la comunicación como lo son la telefonía y la televisión.

El presente trabajo de titilación apunta a la necesidad de mejorar los servicios ya utilizados de la telefonía IP, que es una tecnología que cada día aumenta mas la cantidad de gente que la utiliza, ya que la red Internet cada ves cuenta con mas ancho de banda y mejor capacidad para asegurar la calidad de una llamada a través de la red IP.

La voz sobre IP corresponde a la transmisión de una señal de voz sobre la red IP existente en todo el mundo, permitiendo la comunicación a grandes distancias, lo que se traduce en una disminución del costo monetario de la llamada, ya que se esta utilizando la misma red par varios servicios. Sin contar el hecho que si estamos en presencia de una red LAN corporativa, las llamadas que se realicen dentro de esta red son gratis en su totalidad, ya que solo corresponde al tráfico de información dentro de la red interna de la compañía. El costo de una llamada de telefonía IP se traduce en la utilización de Gateways para la conexión de una red Pública conmutada, con una red IP, como también la utilización de más de una RED LAN corporativa, atravesando la voz en más de un Router.

Esta tecnología, capta cada día mas clientes gracias a la calidad de la transmisión de la voz dentro de la red IP, lo que se llama el QoS (Calidad de servicio), cosa que en la versión actual del protocolo IP (IPv4), no esta asegurada la calidad de servicio para las llamadas de voz en la red, pero el nuevo protocolo IPv6, si tiene asegurada la calidad de servicio junto con muchas otras grandes ventajas que supera en gran medida al antigua versión de protocolo IP. Es por esto que en el proyecto de titulación se contempla la comunicación de un equipo que se encuentre en la antigua versión de IP (IPv4) y uno en la Nueva versión del protocolo IP (IPv6), como también el estudio de la maximización de recursos de los router inalámbricos presentes en el mercado, para así lograr una topología robusta, compacta y acorde a la época que estamos viviendo, de gran desarrollo y aparición de nuevas oportunidades para todo lo referente a las redes IP.

CAPITULO I
ESTADO DEL ARTE DE LA VOIP

1.1 Antecedentes

Lo que se conocía como la telefonía ha tenido grandes avances a través del tiempo, desde sus principios con los experimentos de la telegrafía de Marconi (1874 – 1937) hasta la actualidad, con los avances que ha tenido la informática y las telecomunicaciones en un mundo globalizado, las cuales hoy nos permite la comunicación a través de Internet y el envío de paquetes de voz a través de redes de datos (redes IP), que es lo que hoy denominamos La Voz sobre IP (VoIP).

En lo que respecta al tema específico de la VoIP, este comenzó como el resultado del trabajo de un grupo de jóvenes en Israel durante el año 1995. En aquella época, la única comunicación existente que era posible es la de PC-a-PC. Poco más tarde Vocaltec, anunció el lanzamiento del primer Softphone que llamaron “Internet Phone Software”. Este Softphone estaba hecho para ser usado en un PC que tenía solo tarjeta de sonido, micrófono, parlantes y modem. El software funcionaba comprimiendo la señal de voz, convirtiéndola en paquetes de voz que eran enviados por Internet (exactamente igual que hoy). El software sólo funcionaba si los dos PC tenían el mismo software y el mismo hardware. Lo que por motivos evidentes fue comercialmente un gran fracaso, principalmente porque las comunicaciones de banda ancha todavía no estaban disponibles, como lo es en la actualidad.

Ya en el año 1997 Jeff Pulver decide juntar por primera vez a los pocos usuarios, fabricantes, e interesados en esta tecnología en VON, la primer feria/congreso que actualmente sigue siendo el mayor evento de VoIP. Ahora Pulver organiza VON, 2 veces por año en EEUU, y ahora también una vez por año en varios países de Europa. También formó una compañía prestadora de servicio VoIP llamada FreeWorldDialup comúnmente llamada FWD (que puede confundirse con el término FWD = transferencia de llamadas) y es co-fundador de Vonage, el proveedor de VoIP más grande de EEUU. Pulver tiene varias empresasrelacionadas con VoIP,

entre ellas PulverMedia, su empresa encargada de organizar VON y publicar medios en todo el mundo.

En 1998 la VoIP dio otro gran salto. Un grupo de emprendedores comenzó a fabricar los primeros ATA/Gateways para permitir las primeras comunicaciones PC-a teléfono convencional y, finalmente, las primeras comunicaciones teléfono-convencional - a - teléfono-convencional (con ATAs en cada extremo). Algunos de estos emprendedores inicialmente daban el servicio sin cargo a sus clientes para que pudieran probar la calidad y la tecnología. Estas llamadas contenían publicidad en el inicio y al final de cada comunicación. Estos servicios sólo se prestaban en EEUU y funcionaban gracias a esta publicidad. A menudo debía comenzarse la comunicación a través de una PC para luego pasar a un teléfono convencional. En este punto VoIP sumaba el 1% del total del tráfico de voz. Durante 1998 tres fabricantes comenzaron a fabricar switches de Capa 3 con QoS.

En 1999, Cisco vende sus primeras plataformas corporativas para VoIP. Se utilizaba principalmente el protocolo H.323 de señalización. En el año 2000 VoIP representaba más del 3% del tráfico de voz. El mismo año Mark Spencer un estudiante de la Universidad de Auburn crea Asterisk, la primer central telefónica / conmutador basada en Linux con una PC personal con un código fuente abierto. Asterisk hoy ofrece una solución freeware para hogares/pequeñas empresas y soluciones IP-PBX corporativas. Mark Spencer es el CEO de Digium.

En 2002 el protocolo SIP comienza a desplazar al H.323. En 2003 dos jóvenes universitarios - Jan Friis y Niklas Zenntrom - crean un softphone gratuito fácilmente instalable en cualquier PC que puede atravesar todos los firewalls y routers inclusive los corporativos. Ese producto es Skype, que se propaga con una velocidad increíble y llega en diciembre de 2005 a contar con 50 millones de usuarios.

La evolución y desarrollo que ha tenido VoIP, tiende a desplazar el sistema de teléfonos tradicionales por teléfonos IP. Lo anterior, si se tiene en cuenta que poco a poco todo el mundo cambiará sus teléfonos tradicionales por teléfonos IP apoyados por las propias operadoras de telefonía y servicios IP. Pero hay que destacar que el camino a seguir por parte de los investigadores de voz sobre IP no ha sido fácil, pues han encontrado inconvenientes a través de

su proceso investigativo que, de una u otra forma, han contribuido para que el proyecto no se haya llevado a cabalidad ni desarrollado a un punto más alto; algunos de estos factores, que han sido determinantes en el avance de esta tecnología, se relacionan a continuación:

- El constante freno que han aplicado las empresas de telefonía existentes, valiéndose de herramientas de tipo jurídicas.
- El afán de las grandes compañías telefónicas por adueñarse de esta tecnología para sacar el mejor provecho.
- El alto costo de los DSP's (Procesador Digital de señal).

1.1.1 ¿Qué es la VoiP?

La VoIP (Voz sobre IP), Voz sobre Protocolo de Internet, o también llamada Telefonía IP se puede definir como la transmisión de paquetes de voz utilizando redes de datos en lugar de enviarla en forma de circuitos como una compañía telefónica convencional o PSTN. La comunicación se realiza por medio del protocolo IP (Internet Protocol), permitiendo establecer llamadas de voz y fax sobre conexiones IP (Redes de Datos Corporativos, Intranets, Internet, etc.), obteniendo de esta manera una reducción de costos considerables en la telefonía. Esta definición expresa muy generalmente lo que corresponde a la VoIP, pero si requerimos ahondar a algo mucho mas detallado y rigurosamente estudiado, debemos analizar muchos tópicos, estándares y protocolos que se utilizan dentro de la comunicación a través de la red IP.

Existen varias definiciones, todas concluyen en un punto importante: Envío de voz comprimida y digitalizada en paquetes de datos y sobre protocolo de Internet (IP), utilizando redes de datos aprovechando el ancho de banda que ofrece y el cableado, ahorrando costos importantes para las empresas.

Cabe señalar que la definición de la Telefonía IP es un poco distinta que la VoIP, aunque signifiquen exactamente los mismo en el echo de la comunicación, pero la Telefonía IP se puede definir como el uso de paquetes IP para tráfico de voz fullduplex. Estos paquetes son transmitidos

a través de Internet o de redes IP privadas. El componente clave de la tecnológica en telefonía IP son los equipos que convierten la señal de voz analógica en paquetes IP. Estos equipos pueden ser tarjetas específicas para PC, software específico o servidores-pasarela de voz.

El Protocolo Internet en un principio se utilizó para el envío de datos, actualmente debido al creciente avance tecnológico, es posible enviar también voz digitalizada y comprimida en paquetes de datos, los cuales pueden ser enviados a través de Frame Relay, ATM, Satélite, etc. Una vez que estos paquetes llegan a su destino son nuevamente reconvertidos en voz.

1.1.2 ¿Que Ofrece el Mercado?

En el mercado de la voz sobre IP, se encuentra una serie de ofertas en elementos que nos permitirán construir aplicaciones para la VoIP. Alguno de ellos, y los más importantes son:

1. Teléfonos IP.
2. Adaptadores para PC.
3. Hubs Telefónicos.
4. Gateways (pasarelas RTC / IP).
5. Gatekeeper.
6. Unidades de audio conferencia múltiple. (MCU Voz)
7. Servicios de Directorio.

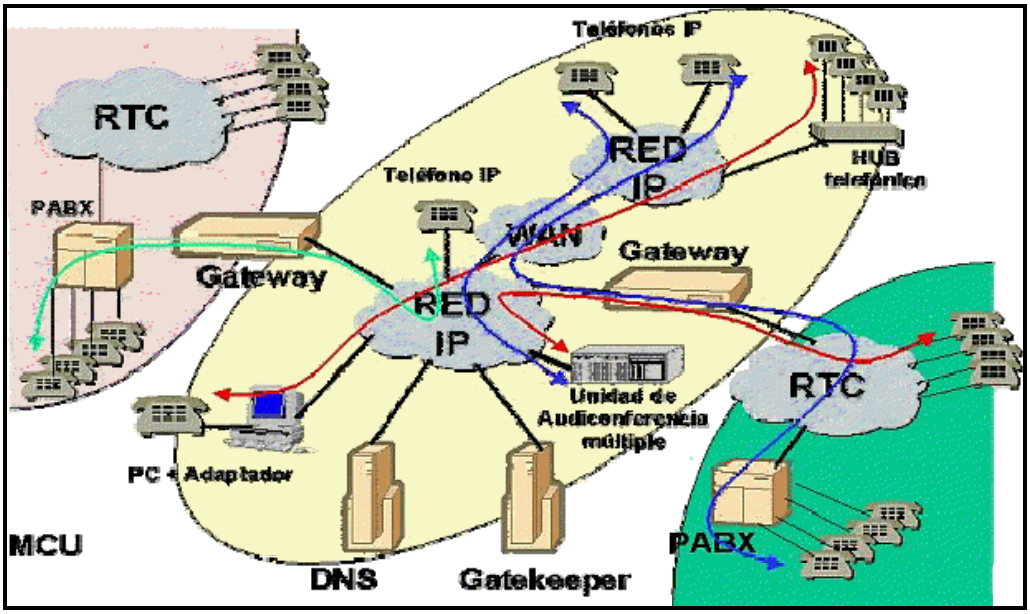


Figura Nº 1.1: Elementos de una red de VoIP

Todos estos elementos los podemos ver en la figura 1.1, la cual muestra una red convencional de VoIP que se conecta a la red de telefonía tradicional o RTC (red de telefonía conmutada). Unos de los elementos mas importantes de la VoIP son los Gatekeeper y los Gateway, ya que la presencia de ellos dentro de la red son de gran relevancia y sus tareas a desarrollar los conviertes en elementos claves en las redes de VoIP comerciales, una descripción breve de ellos a continuación:

- El **Gatekeeper** es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de este. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación en la misma.
- El **Gateway** es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI (Red Digital de Servicios Integrados). Podemos considerar al Gateway como una caja que por un lado tiene un interfase LAN y por el otro dispone de uno o varios de los siguientes interfaces:
  - FXO. Para conexión a extensiones de centralitas o a la red telefónica básica.
  - FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.

- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI (2B+D)
- PRI. Acceso primario RDSI (30B+D)
- G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps.

1.1.3 Aspectos importantes de la VoIP

Uno de los aspectos más importantes que se debe mencionar cuando se habla de VoIP, es el hecho que la voz presenta retardos en su transmisión. De hecho, si el retardo introducido por la red es de más de 300 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico.

Siempre debemos tener presente que los paquetes IP son tramas de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP (Protocolo de Reservación de Recursos), cuya principal función es dividir los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un ruteador. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM que proporcionan QoS de forma estándar.

Los servicios de telefonía IP no están limitados a los usuarios de PCs con acceso a Internet, ya que mediante la colocación de los dispositivos gateway, los proveedores de servicio pueden ofrecer servicios de telefonía IP. Ya que existen tres componentes en la tecnología de la telefonía IP: Clientes, servidores y gateways (puertas de acceso), los cuales nos permiten una amplia comunicación entre dispositivos, tanto de telefonía tradicional como de telefonía IP. Una descripción de estos tres componentes son:

- **El cliente**
  - Establece y termina las llamadas de voz; Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario.
  - Recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario.
  - El cliente se presenta en dos formas básicas.

    1. Una suite de software corriendo en una PC que el usuario controla mediante una interfaz gráfica de usuario (GUI)
    2. Puede ser un cliente "virtual" que reside en un gateway.

- **Los servidores**
  - Manejan un amplio rango de operaciones, las cuales incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección y distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios, servicios de directorio y otros.

- **Los gateways de telefonía IP**
  - Proporcionan un puente entre los mundos de la telefonía tradicional y la telefonía sobre Internet; es decir, permiten a los usuarios comunicarse entre sí. La función principal de un gateway es proveer las interfaces apropiadas para la telefonía tradicional, funcionando como una plataforma para los clientes virtuales. Los gateways juegan también un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS) y en el mejoramiento del mismo. Es por esto que la telefonía IP no solo se restringe a usuarios que cuenten en sus hogares con PCs, si no que tan solo con un gateway a disposición ya tienen acceso a los servicios de telefonía IP los teléfonos convencionales de telefonía.

    La conversión de la voz a datos requiere una sofisticada formulación matemática, que comprime la voz humana digitalizada en un conjunto de datos mucho más

pequeño y manejable. Una fórmula similar expande los datos comprimidos para devolver la voz a su estado original una vez que llega a su destino, minimizando el ancho de banda consumido, por lo que se optimizan los recursos disponibles. Por ejemplo, una conversación de telefonía IP ocupa aproximadamente la octava parte que una tradicional. Es por esto y gracias a que las formulaciones matemáticas y los procesadores de señal para la compresión y descompresión de la voz en datos son cada vez más eficientes, y los anchos de banda disponibles para el traslado de la voz sobre IP cada vez son mayores, la calidad de las comunicaciones de voz sobre IP ha superado la de la telefonía celular, y prácticamente ha igualado a la de las llamadas telefónicas sobre sistemas de telefonía estándar.

1.2 Redes Públicas vs. Redes de datos.

Uno de los tipos de redes públicas es la Red telefónica pública conmutada (PSTN.- Public Switched Telephone Network), de la cual existen 600 millones de usuarios alrededor del mundo y su tráfico de voz se incrementa a una velocidad del 8% anual.

Otro de los tipos existentes y una de las más conocidas es la Red de paquetes INTERNET con más de 100 millones de usuarios de Internet alrededor del mundo, con un tráfico de datos que se incrementa a una velocidad anual del 35%.

El tráfico de datos predice que avanza más rápido que el tráfico de voz (bits/seg) 2000–2002. Como lo muestra la gráfica de la figura 1.1.

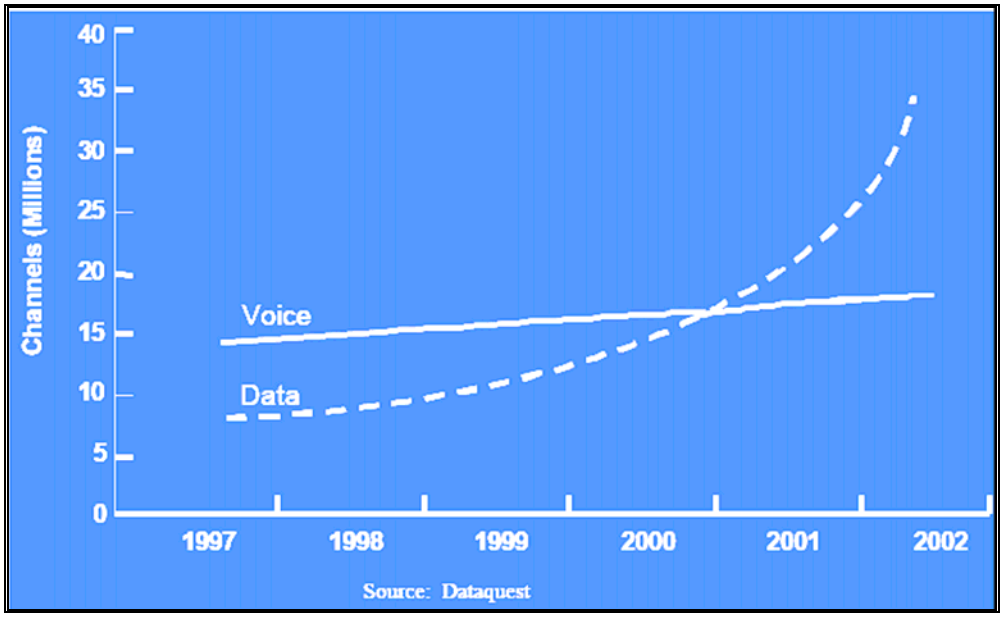


Figura 1.2: Canales de Voz vs. Datos

Las redes de telefonía pública han transmitido datos utilizando:

- Modems.
- ISDN-T1
- Frame Relay

Por otro lado las redes de datos están empezando a transmitir voz, como es el caso de:

- Voz sobre IP.
- Voz sobre frame relay.

Aunque actualmente el uso de las redes sea el envío conjunto de voz y datos, tanto las redes de telefonía pública como las redes de datos fueron creadas con características propias, las cuales se resumen en la tabla 1.1

CARACTERÍSTICAS DE LAS REDES DE VOZ.	**CARACTERÍSTICAS DE LAS REDES DE PAQUETES DE DATOS.**
1) Están diseñadas para llevar voz en tiempo real.	1) Están diseñadas para transferencia de archivos.

2) Cuentan con circuitos conmutados. a) Circuito de múltiple switcheo coordinando una sola ruta de llamada. b) Rutas dedicadas. c) Circuitos para llamadas punto a punto. 3) Formato PCM sincrono de 64 Kbit. 4) Diseño de lento retardo (<50ms).	2) Paquetes conmutados. a) Paquetes enrutados individualmente b) Cada router direcciona cada paquete separadamente. 3) Formato: Protocolos de paquetes TCP/IP y UDP. 4) El control de retardo no es problema.
	➢ TCP/IP diseñado para compartir archivos. ➢ Conexiones: - Cada paquete tiene una dirección de destino. - Cada paquete toma su propia ruta. - Los paquetes se pueden obtener fuera de secuencia. - Mejor esfuerzo de entrega. - Retransmisión de paquetes sobre errores

Tabla 1.1: Redes de Voz vs. Redes de Datos

1.3 Problema de Retado y Solución para la VoIP.

Los requerimientos básicos para el transporte de la voz sobre una red de datos (red IP), se pueden resumir en los siguientes:

- Tiempo de entrega garantizado. (Máximo retardo en una ruta, 150 ms.)
- Tasa de calidad de voz en nivel PCM ó mejor.
- Señalamiento de tono (DTMF).

Según estos requerimientos aparece uno de los grandes problemas que tiene la VoIP, aunque ha sido mejorado y cada día es menor, el retardo sigue siendo el gran miedo de las granes empresas a utilizar esta herramienta para trasladar la voz en sus redes de datos.

Ahora, este retardo aparece por las siguientes causas:

- Paquetes fuera de secuencia.
- Pérdida de paquetes
  - La Retransmisión causa retardos extensivos.
  - No hay opción de retransmisión.
  - TCP/IP no es útil para voz interactiva.
  - Retardos de codificación.
  - Retardo de paquetización.
  - Retardo de transporte.
  - Retardo de ruteo.

También podríamos decir que básicamente, los problemas principales de la transmisión de voz a través de Internet son: ancho de banda limitado (aunque cada día las ofertas en el mercado aumentan la posibilidad de un ancho de banda mayor, y con las redes gigabit ethernet, esto es casi despreciables) y latencia impredecible. Mediante algoritmos de compresión de voz se consigue que el ancho de banda necesario sea mínimo. La latencia, (el retardo que se produce debido a la digitalización, compresión y paquetización de la voz y el hecho de que los paquetes deban atravesar diversos ruteadores y líneas) exige que los paquetes de voz lleguen a velocidad constante, a pesar de que el oído humano tolere la perdida de paquetes. La latencia se disminuye mediante la utilización de tarjetas digitalizadoras específicas (DSP's) o mediante la utilización de software y procesadores veloces.

En la figura 1.3 se puede apreciar detalladamente el recorrido que realizan los paquetes de voz así como los tiempos de retardo en el transporte.

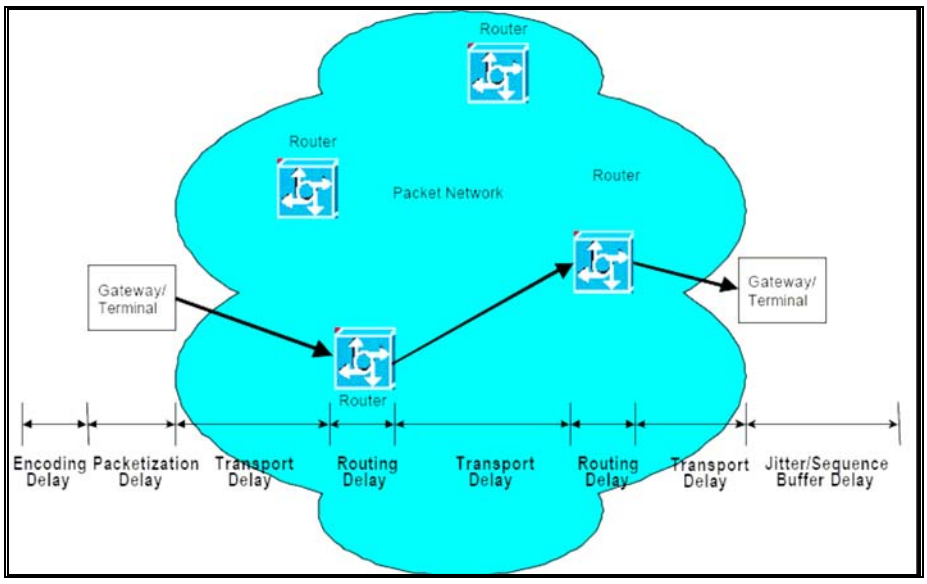


Figura 1.3: Balance del retardo en el transporte de voz

La tabla 1.2 muestra los retardos que presentan las diferentes normas de compresión VoIP.

Vocoder	MOS	Bandwidth	Complexity	delay
G.711	4.4	64	<1 MIPS	~1ms
G.723.1	3.4/3.6	5.4/6.3	21 MIPS	37.5ms
G.729A	4.0	8	11 MIPS	15ms
GSM 6.10	3.1	13	8 MIPS	27.5ms

Tabla 1.2: Vocorder Encoding Delay

En el año 2000, el ingeniero Ellis K. Cave en su conferencia New Directions in IP Telephony, mencionó que los problemas de retardo en voz pueden tener solución si se toman en cuenta los siguientes puntos:

1. *Dar más ancho de banda.*

Al ofrecer más ancho de banda el problema de retardo no se garantiza, siempre existe probabilidad para colisiones, se requiere un gran tamaño de ancho de banda en la red para manejar todas las llamadas sin congestión.

2. *Dar un protocolo de retardo garantizado sobre los protocolos de paquetes existentes, es decir, se requiere un protocolo para:*

    i. Reservación de recursos (RSVP, SII), que permita una específica QoS para cada aplicación.
    ii. Requiere modificación de rutas actuales para nuevos protocolos (ej. multicast)
    iii. El reservado de ancho de banda se obtiene del usuario final, del proveedor de accesos y proveedor de red; es aquí donde surge una interrogante ¿Quién y como paga estos recursos?

3. *Trazar un nuevo protocolo que incluya problemas de retardo:*

    i. Modo de transferencia asíncrona (ATM): ATM puede trabajar tráfico asíncrono y tráfico en ráfagas y proporcionar la calidad de servicio (QoS) solicitada. Combina los beneficios de la conmutación de paquetes y la conmutación de circuitos, reservando ancho de banda bajo demanda de una manera eficaz y de costo efectivo, a la vez que garantiza ancho de banda y calidad de servicio para aquellas aplicaciones sensibles a retardos como lo es VoIP.
    ii. Compromiso entre requerimientos de voz y datos.
    iii. Dándole la misma importancia a la tarifación.

1.4 Arquitectura del Protocolo VoIP

Después de haber constatado que se pueden comunicar dos PC con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, pero para realizar estas llamadas intervienen una serie de protocolas y estándares, siendo los protocolos de comunicación mas utilizados el SIP, H.323 y los de transporte RTCP, RTP, RTSP. A continuación la figura 1.4 muestra la estructura de los protocolos mencionados anteriormente

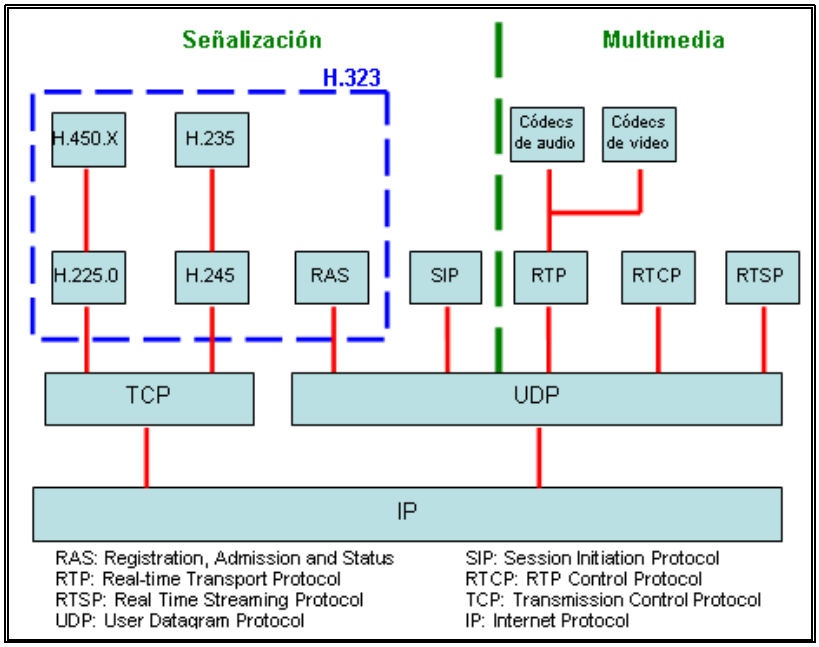


Figura 1.4: Estructura de Protocolo de VoIP

El VoIP/H.323 comprende a su vez una serie de **estándares** y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:

  1. RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.
  2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

- Señalización:

  1. Señalización inicial de llamada.
  2. H.225 Control de llamada: señalización, registro y admisión, paquetización / sincronización del flujo de voz.

3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para flujos de voz

- Compresión de voz:

1. Requeridos: G.711 y G.723.
2. Opcionales: G.728, G.729 y G.722

- Transmisión de voz:

1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

- Control de la transmisión:

RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

La tabla 1.3 visualiza gráficamente el nivel en el que trabajan estos protocolos cuando se establece una llamada VoIP.

<table>
<tr><td colspan="6">Establecimiento de llamada y Control</td></tr>
<tr><td colspan="2"></td><td colspan="2">Presentación</td><td colspan="2"></td></tr>
<tr><td colspan="2">Direccionamiento</td><td colspan="2">Compresión de audio G.711 ó G.723</td><td>DTMF</td><td>Direcciona-miento</td></tr>
<tr><td>RAS(H.225)</td><td>DNS</td><td colspan="2">RTP/RTCP</td><td>H.245</td><td>Q.931 (H.225)</td><td>DNS</td></tr>
<tr><td colspan="3">Transporte UDP</td><td colspan="3">Transporte TCP</td></tr>
<tr><td colspan="6">Red (IP)</td></tr>
<tr><td colspan="6">Enlace</td></tr>
<tr><td colspan="6">Físico</td></tr>
</table>

Tabla 1.3: Pila de protocolos VoIP

El hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir. Una idea que parece inmediata es que el papel tradicional de la centralita telefónica quedaría distribuido entre los distintos elementos de la red VoIP. En este escenario, tecnologías como CTI (computer-telephony e integration) tendrán una implantación mucho más simple. Será el paso del tiempo y la imaginación de las personas involucradas en estos entornos, los que irán definiendo aplicaciones y servicios basados en VoIP.

A continuación se realizara una explicación de estas dos clases de protocolos (Señalización y Multimedia) poniendo énfasis en sus diferencias y sus características más importantes. Adicionalmente, se compararán los diversos *codecs* usados en los protocolos de transporte. En el presente trabajo de titulación se utilizara el término *codec* como abreviatura de Codificador-DECodificador de señales de voz, es decir, convierte la señal de voz en un flujo de datos para que pueda viajar por algún medio de transporte. En esta tesis, el medio de transporte es la red IP de la RAAP.

1.4.1 Protocolos de señalización.

VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

De acuerdo a la UIT en su recomendación H.323 [UIT2003], el protocolo de señalización se encarga de los mensajes y procedimientos utilizados para establecer una comunicación, pedir cambios de tasa de bits de la llamada, obtener el estado de los puntos extremos y desconectar la llamada.

1.4.1.1 H.323

Normado por la ITU (Unión Internacional de Telecomunicaciones) H.323 es un estándar que norma todos los procedimientos para lograr Sistemas Audiovisuales y Multimedios, por lo que engloba varios protocolos y estándares. Uno de estos procedimientos es la señalización de la llamada

Aprobado en octubre de 1996, el estándar H.323 soporta multimedia sobre Ethernet, Fast Ethernet, FDDI y LANs Token Ring. En el contexto de H.323 las LANs también incluyen redes formadas por múltiples LANs interconectadas por conmutadores, puentes y routers. H.323 es una especificación significativa porque permite el desarrollo de una nueva generación de aplicaciones multimedia basadas en LAN.

La versión 2 de H.323, aprobada en febrero de 1998, añade incluso más funciones en las áreas de servicios complementarios, seguridad y protocolo de RAS (registro, admisión y estatus).

H.323 define cuatro componentes principales para un sistema de conferencia multimedia basado en LAN: Terminales, pasarelas, unidades de control multipunto (multipoint control units, MCUs) y gatekeepers. Las terminales, las pasarelas y los MCUs son considerados extremos porque pueden generar y/o terminar sesiones H.323. El gatekeeper es considerado una entidad de red porque no puede ser llamado, pero se le puede solicitar que lleve a cabo funciones específicas tales como traducción de direcciones o control de acceso. Cada componente se describe a continuación.

1.4.1.1.1 Terminal H.323

.

Todas las implementaciones H.323 han de tener, como mínimo, codec de audio G.711, controles de sistemas y nivel H.224, ésta recomendación no incluye especificaciones para el interfaz de LAN.

H.245 define los mensajes de control que soportan señalización extremo a extremo entre dos puntos. H.245 especifica la sintaxis y la semántica exactas que implementan el control de llamadas, comandos e indicaciones generales, la apertura y cierre de canales lógicos, la determinación de retardos, los requisitos de preferencias de modo, los mensajes de control de flujo y los intercambios de capacidad.

H.225 proporciona el servicio multiplex y demultiplex empleado por H.323. Es responsable de paquetizar y sincronizar las corrientes de audio, video, datos y control para su transmisión por el interfaz de LAN.

1.4.1.1.2 Gateway H.323

Como su nombre sugiere, una pasarela es un sistema que proporciona entrada a una red y salida de una red. Las pasarelas son las responsables de traducir el control del sistema, los codecs de audio y los protocolos de transmisión entre los diferentes estándares ITU.

La tabla 1.4 muestra los pasos en una secuencia de arranque de una sesión H.323 típica.

Acción	Protocolo H.323	Protocolo de transporte
El extremo solicita al gatekeeper permiso y ancho de banda para comenzar una sesión H.323.	RAS	UDP
Los extremos negocian y establecen la configuración de llamada.	Q.931	TCP
Los extremos intercambian capacidades y restablecen los canales RTP.	H.245	TCP
Los extremos intercambian datos de audio.	H.225	UDP

Tabla 1.4: Secuencia de arranque de una sesión H.323 típica.

Dada la gran cantidad de redes que utilizan IP, la mayoría de las implementaciones H.323 estarán basadas en IP. Por ejemplo, la mayor parte de las aplicaciones de telefonía IP están basadas en la configuración H.323 mínima que incluye codec de audio, control del sistema y componentes de red. H.323 requiere un servicio TCP extremo a extremo fiable para documentar y controlar las funciones. Sin embargo, utiliza un sistema no fiable para transportar información de audio y video. H.323 se basa en el Protocolo de Tiempo Real (Real-time Protocol, RTP) y el Protocolo de Control de Tiempo Real (Real-Time Control Protocol, RTCP) por encima de la UDP para ofrecer corrientes de audio en redes basadas en paquetes.

Ahora, si vemos al protocolo H.323desde el punto de vista de la señalización, este protocolo nos propondría dos tipos de señalización [PAC2006]:

- ***Señalización de control de llamada (H.225.0):*** Este protocolo tiene dos funcionalidades. Si existe un *gatekeeper* en la red, se define como un terminal y se

Status) y usa un canal separado (canal RAS). Si no existiese un *gatekeeper*, se define la forma como dos terminales pueden establecer o terminar llamadas entre sí (Señalización de Llamada). En este último caso se basa en la recomendación Q.931.

- ***Señalización de control de canal (H.245):*** Una vez que se ha establecido la conexión entre dos terminales usando H.225, se usa el protocolo H.245 para establecer los canales lógicos a través de los cuales se transmite la media. Para ello define el intercambio de capacidades (tasa de bits máxima, *codecs*, etc.) de los terminales presentes en la comunicación.

Se usa RAS siempre y cuando un *Gatekeeper* esté presente en la red. El *Gatekeeper* es un componente opcional cuya función principal es el control de admisión. Es un intermediario entre los puntos terminales que permite el establecimiento de llamadas entre estos. También puede enrutar la señalización hacia otro dispositivo para implementar funciones como desvío de llamadas.

Una llamada H.323 se caracteriza por las siguientes fases de señalización [MAR2006]:

- **Establecimiento de la comunicación.** Primero se tiene que registrar y solicitar admisión al *Gatekeeper*, para lo cual se usan los mensajes RAS. Luego, el usuario que desea establecer la comunicación envía un mensaje de SETUP, el llamado contesta con un mensaje de *CallProceeding*. Para poder seguir con el proceso, este terminal también debe solicitar admisión al *GateKeepe*r con los mensajes RAS y, una vez admitido, envía el *Alerting* indicando el inicio del establecimiento de la comunicación. Este mensaje *Alerting* es similar al *Ring Back Tone* de las redes telefónicas actuales. Cuando el usuario descuelga el teléfono, se envía un mensaje de *Connect*.

- **Señalización de Control.** En esta fase se abre una negociación mediante el protocolo H.245 (control de canal). El intercambio de los mensajes (petición y respuesta) entre los

dos terminales establece quién será maestro y quién esclavo, así como también sus capacidades y los *codecs* de audio y video soportados (Mensajes TCS, *Terminal Capability Set*). Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto) (Mensajes OLC, *Open Logical Channel*).

- **Audio:** los terminales inician la comunicación mediante el protocolo RTP/RTCP.

- **Desconexión.** Por ultimo, cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante los mensajes *Close Logical Channel* (CLC) y *End Session Command* (ESC). Una vez hecho esto, ambos terminales tienen que informarle al *Gatekeeper* sobre el fin de la comunicación. Para ello se usan los mensajes RAS DRQ (*Disengage Request*) y DCF (*Disengage Confirm*).

Ya en la figura 1.5 se puede observar con más detalle las fases de una llamada con el protocolo H.323:

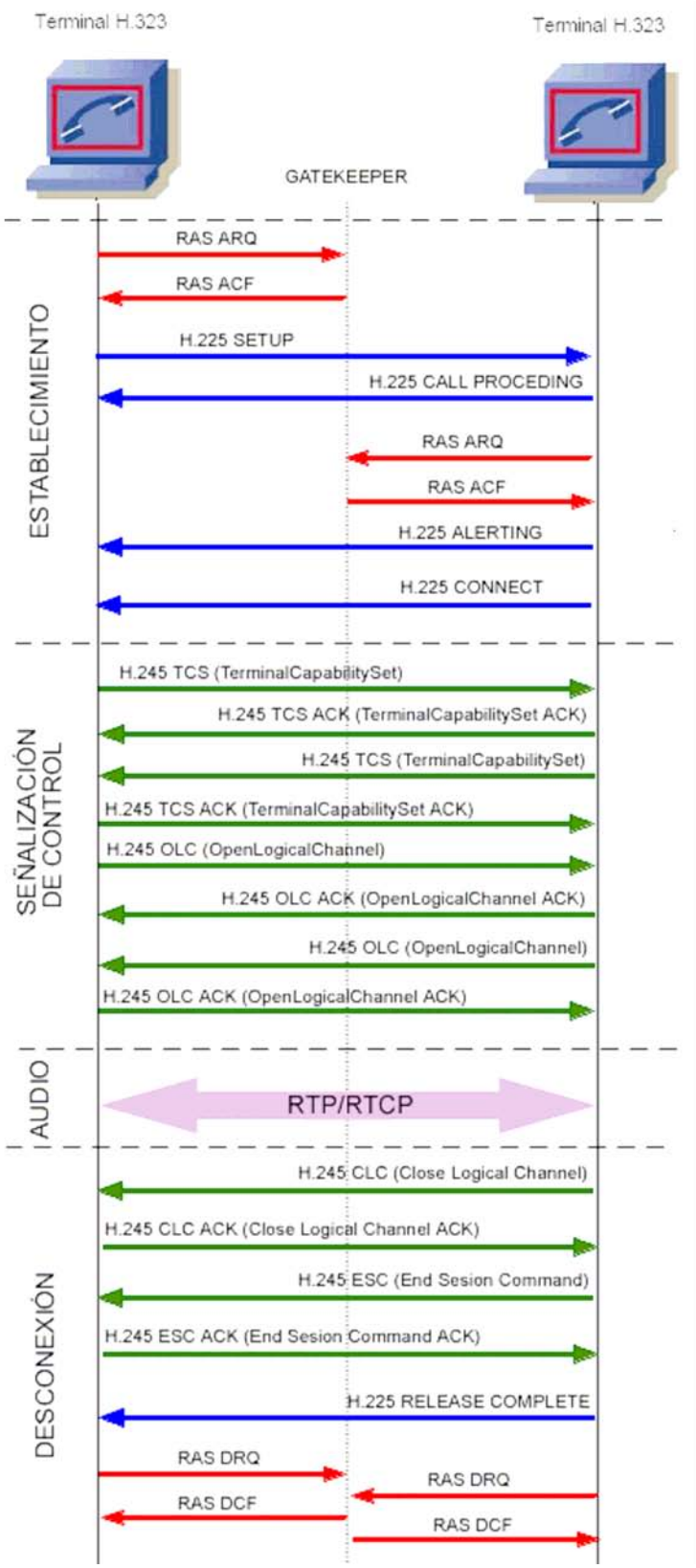


Figura 1.5: fases de una llamada H.323

1.4.1.2 SIP (Session Initiation Protocol)

A diferencia de H.323, SIP tiene su origen en la comunidad IP, específicamente en la IETF (*Internet Engineering Task Force*); y no en la industria de las Telecomunicaciones (UIT).

SIP es similar al HTTP en muchos sentidos, incluso tiene algunos mensajes de error en común, como el “404 no encontrado” (*404 not found*) y el “403 servidor ocupado” (*403 Server Busy*).

Los componentes presentes en SIP son:

1. Agentes de Usuario (*User Agent*, UA): Existen dos tipos de agentes de usuario, los cuales están presentes siempre, y permiten la comunicación cliente-servidor:

    a. Agente de usuario cliente (UAC): El UAC genera peticiones SIP y recibe respuestas.
    b. Agente de usuario servidor (UAS): El UAS responde a las peticiones SIP.

2. Servidores SIP: Existen tres clases lógicas de servidores. Un servidor puede tener una o más de estas clases. Estas clases son las siguientes:

    a. Servidor de Redirección (*Redirect Server*): Reencamina las peticiones que recibe hacia el próximo servidor.
    b. Servidor Proxy (*Proxy Server*): Corren un programa intermediario que actúa tanto de servidor como de cliente para poder establecer llamadas entre los usuarios.
    c. Servidor de Registro (*Registrar Server*): Hace la correspondencia entre direcciones SIP y direcciones IP. Este servidor solo acepta mensajes REGISTER, lo que hace fácil la localización de los usuarios, pues el usuario donde se encuentre siempre tiene que registrarse en el servidor.

Se define dos tipos de mensajes SIP: Peticiones y Respuestas.

1. Peticiones SIP. Se definen 6 métodos básicos:

    a. ***INVITE***: Permite invitar un usuario a participar en una sesión o para modificar parámetros de una sesión ya existente.
    b. ***ACK:*** Confirma el establecimiento de la sesión.
    c. ***OPTION:*** Solicita información de algún servidor en particular.
    d. ***CANCEL:*** Cancela una petición pendiente.
    e. ***REGISTER:*** Registra al Agente de Usuario.

2. Respuestas SIP: Existen también mensajes SIP como respuesta a las peticiones. Existen 6 tipos de respuestas, que se diferencian por el primer dígito de su código. Estas son:

    a. 1xx: Mensajes provisionales.
    b. 2xx: Respuestas de éxito.
    c. 3xx: Respuestas de redirección.
    d. 4xx: Respuestas de fallas de método.
    e. 5xx: Respuestas de fallas de servidor.
    f. 6xx: Respuestas de fallas globales.

Algunos de los mensajes que se dieron a conocer anteriormente, los podemos apreciar en el ejemplo de comunicación ilustrado en la figura 1.6, que corresponde a un intercambio de mensajes bajo el protocolo SIP.

Cabe mencionar que para el desarrollo de este trabajo de titilación, se utilizara el protocolo SIP y luego en el capitulo III, se explicaran la forma en que se utiliza y con que programa se esta utilizado dentro del AP.

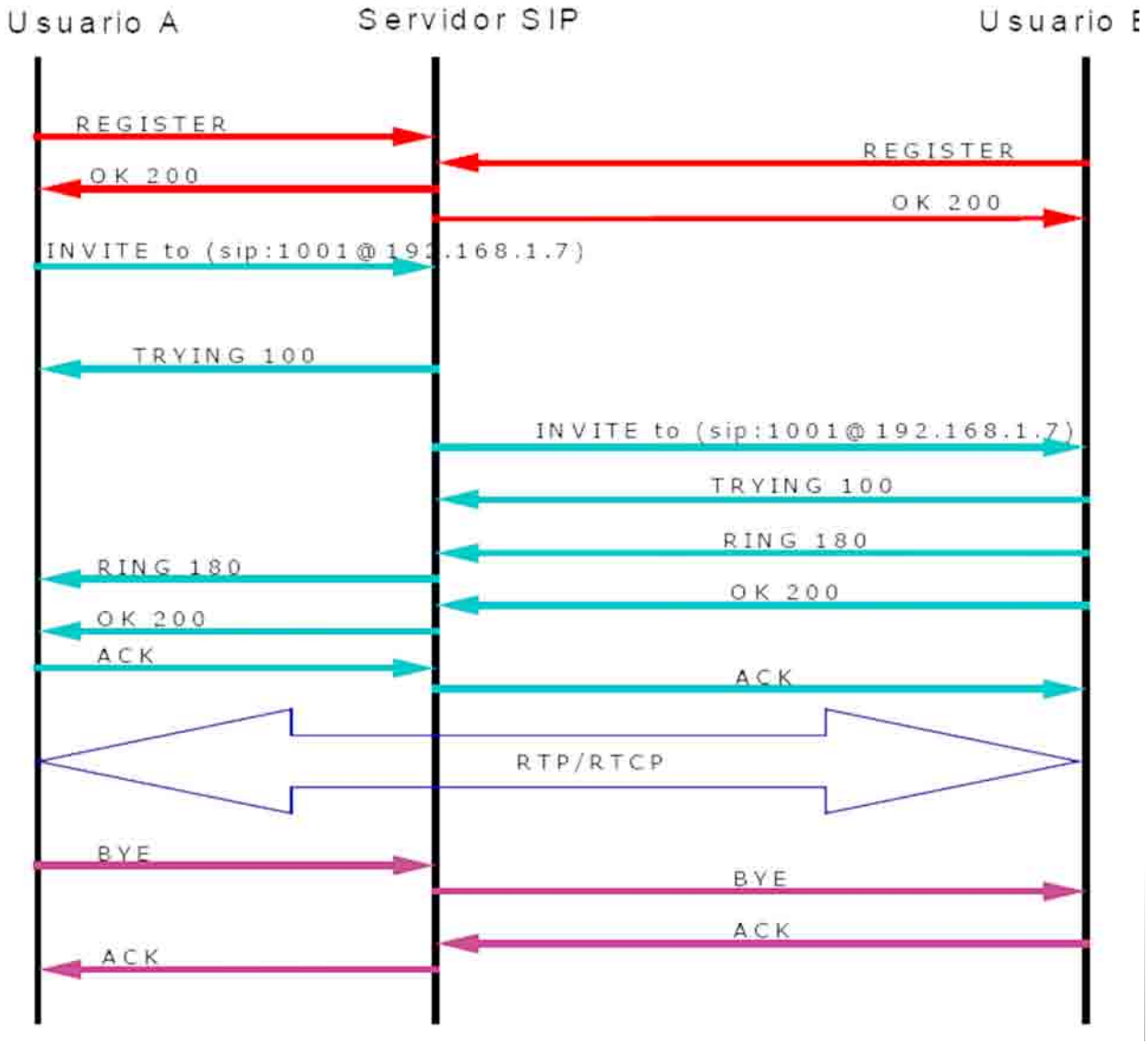


Figura 1.6: Intercambio de mensajes en SIP

Las dos primeras transacciones tienen que ver con el registro de usuarios. El punto medio es el servidor que en esta etapa actúa como servidor de registro.

La siguiente transacción establece el inicio de sesión. El Usuario A (llamante) le manda un INVITE al Usuario B (llamado) a través del servidor, que redirecciona la llamada a este último. La sesión se establece cuando ambos puntos mandan la confirmación.

Cuando la sesión se ha establecido, entra a funcionar el protocolo de transporte (RTP, *Real-time Transport Protocol*), que es el encargado del transporte de la voz.

Cuando alguien quiere terminar la comunicación, manda la petición BYE que el servidor lo redirecciona al otro punto. Luego, este último envía la confirmación, terminando así la sesión. Cualquiera de los participantes puede terminar la conversación en cualquier momento.

1.4.1.3 Diferencia entre SIP y H.323

Entre las diferencias lo más importante es la es la velocidad: SIP hace en una sola transacción lo que H.323 hace en varios intercambios de mensajes. Adicionalmente, SIP usa UDP mientras que H.323 debe usar necesariamente TCP para la señalización (H.225 y H.245), lo que origina que una llamada SIP sea atendida más rápido.

Otra diferencia importante es que H.323 define canales lógicos antes de enviar los datos, mientras que una unidad SIP simplemente publicita los *codecs* que soporta, más no define canales, lo que puede generar saturación de tráfico en casos de muchos usuarios, pues no se separa la tasa de bits necesaria para la comunicación.

1.4.1.4 Otros protocolos importantes.

A continuación se analizaran brevemente otros protocolos utilizados en la VoIP, que para el desarrollo de esta tesis no son importantes, pero es recomendable mencionarlos.

1.4.1.4.1 IAX2 (Inter Asterisk Exchange)

Este es el protocolo utilizado por Asterisk. El objetivo con el que se creó este protocolo fue minimizar la tasa de bits requerida en las comunicaciones VoIP y tener un soporte nativo para traspasar dispositivos de NAT (*Network Address Translation*). En

otras palabras, provee soluciones a los problemas dados en SIP y H.323. Fue creado por Mark Spencer, quien también participó en la codificación de Asterisk.

IAX2 usa un único puerto UDP (4569) para transmitir tanto señalización como datos. El tráfico de voz es transmitido en banda (*in-band*), es decir, los datos de voz van encapsulados en el protocolo; SIP, en cambio, se basa del protocolo RTP para la transmisión de los datos (su transmisión es *out-band*). Esto le permite al protocolo IAX2 prácticamente transportar cualquier tipo de dato.

Otra característica de IAX2 es que soporta *Trunking*; es decir, un solo enlace puede enviar datos y señalización de varios canales. Cuando se hace *Trunking*, un solo datagrama IP puede contener información de varias llamadas sin crear latencia adicional. Esto genera una disminución de la tasa de bits y del retraso de los paquetes debido a que ahorra enviar varias veces la cabecera IP.

Todas estas características del IAX2 se deben a que en su diseño se basaron en muchos estándares de señalización y de transmisión de datos, quedándose solo con lo mejor de cada uno. Algunos protocolos tomados como base para el IAX2 son: SIP, MGCP y RTP (Real-time Transfer Protocol).

1.4.1.4.2 *MGCP (Media Gateway Control Protocol)*

Este protocolo está basado en un modelo cliente/servidor, mientras que SIP y H.323 están basados en un modelo peer-to-peer. Este estándar está descrito en [RFC2705], donde se menciona que “este protocolo está diseñado para usarse en un sistema distribuido que se ve desde afuera como un solo gateway VoIP”.

MGCP al igual que SIP usa el Protocolo de Descripción de Sesión (SDP) para describir y negociar capacidades de media. Su funcionalidad es similar a la capacidad H.245 de H.323.

1.4.1.4.3 *SCCP (Skinny Client Control Protocol)*

Protocolo propietario de Cisco, se basa en un modelo cliente/servidor en el cual toda la inteligencia se deja en manos del servidor (*Call Manager*). Los clientes son los teléfonos IP, que no necesitan mucha memoria ni procesamiento [RAM2005]. El servidor es el que aprende las capacidades de los clientes, controla el establecimiento de la llamada, envía señales de notificación, reacciona a señales del cliente (por ejemplo cuando se presiona el botón de directorio). El servidor usa SCCP para comunicarse con los clientes, y si la llamada sale por un *gateway*, usa H.323, MGCP o SIP.

1.4.2 Protocolos de Transporte.

1.4.2.1 RTP (*Real-time Transport Protocol*)

Este protocolo define un formato de paquete para llevar audio y video a través de Internet. Este protocolo no usa un puerto UDP determinado, la única regla que sigue es que las comunicaciones UDP se hacen vía un puerto impar y el siguiente puerto par sirve para el protocolo de Control RTP (RTCP).

La inicialización de la llamada normalmente se hace por el protocolo SIP o H.323. Siendo la idea del trabajo de tesis el trabajar con el protocolo SIP.

El hecho de que RTP use un rango dinámico de puertos hace difícil su paso por dispositivos NAT y *firewalls*, por lo que se necesita usar un servidor STUN (*Simple Traversal of UDP over NAT*). STUN es un protocolo de red que permite a los clientes que estén detrás de un NAT saber su dirección IP pública, el tipo de NAT en el que se encuentran y el puerto público asociado a un puerto particular local por el NAT correspondiente. Esta información se usa para iniciar comunicaciones UDP entre dos *hosts* que están detrás de dispositivos de NAT.

Las aplicaciones que usan RTP son menos sensibles a la pérdida de paquetes, pero son típicamente muy sensibles a retardos, por lo que se usa UDP para esas aplicaciones.

Por otro lado, RTP no proporciona calidad de servicio, pero este problema se resuelve usando otros mecanismos, como el marcado de paquetes o independientemente en cada nodo de la red.

1.4.2.2 RTCP (*Real-time Transport Control Protocol*)

El protocolo de control RTP se basa en la transmisión de paquetes de control fuera de banda a todos los nodos participantes en la sesión. Tiene 3 funciones principales:

- Provee realimentación en la calidad de la data.
- Utiliza nombres canónicos (CNAME) para identificar a cada usuario durante una sesión.
- Como cada participante envía sus tramas de control a los demás, cada usuario sabe el número total de participantes. Este número se usa para calcular la tasa a la cual se van a enviar los paquetes. Más usuarios en una sesión significan que una fuente individual podrá enviar paquetes a una menor tasa de bits.

1.4.3 Codecs

Codec viene de Codificador-Decodificador. Describe una implementación basada en software o hardware para la transmisión correcta de un flujo de datos. Se estudiará solamente los *codecs* de voz.

1.4.3.1 UIT G.711

G.711 tiene una tasa de transmisión alta (64 kbps). Desarrollado por la UIT, es el *codec* nativo de redes digitales modernas de teléfonos.

Formalmente estandarizado en 1988, este *codec*, también llamado PCM, tiene un tasa de muestreo de 8000 muestras por segundo, lo que permite un ancho de banda total para la voz de 4000 Hz. Cada muestra se codifica en 8 bits, luego la tasa de transmisión total es de 64 kbps

Existen dos versiones de este *codec*: Ley-A (A-law) y Ley-μ (μ-law). La segunda se usa en Estados Unidos y Japón mientras que la primera se usa en el resto del mundo, incluida Latinoamérica. La diferencia entre ellas es la forma como la señal es muestreada. Las ecuaciones de muestreo son las siguientes y se grafican en la figura 1.7:

Ley-A:

- $y = \dfrac{Ax}{1 + \ln A}$ para $x \le \dfrac{1}{A}$
- $y = \dfrac{1 + \ln Ax}{1 + \ln A}$ para $\dfrac{1}{A} \le x \le 1$

- Ley-μ:
  - $y = \dfrac{\ln(1 + \mu x)}{\ln(1 + \mu)}$

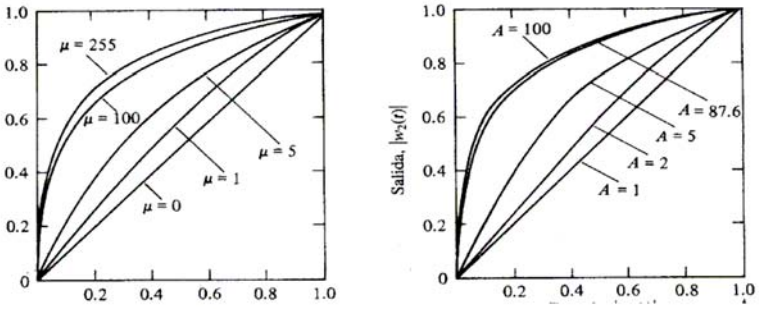


Figura 1.7: COMPARACIÓN LEY-μ VS. LEY-A

Los valores de μ y de A están estandarizados por la UIT y son μ=255 para el caso de la ley-μ y de A=100 para el caso de la ley-A. La forma logarítmica refuerza las muestras más pequeñas de la entrada con el fin de protegerlas del ruido.

El uso de G.711 para VoIP ofrece la mejor calidad (no realiza compresión en la codificación), por lo que suena igual que un teléfono analógico o RDSI. Esto se comprueba con la medida del MOS. El MOS (*Mean Opinion Score*) es una medida cualitativa de la calidad de la voz. Un MOS de 5 indica una comunicación con calidad excelente mientras que un MOS de 0 indica una calidad pésima. G.711 tiene el MOS más alto de todos los *codecs* en condiciones ideales (sin pérdida de paquetes), con un MOS de 4.1.

También presenta el menor retardo debido a que no hay un uso extensivo del CPU (no hay compresión de datos).

El inconveniente principal es que necesita mayor tasa de bits que otros *codecs*, aproximadamente 80 kbps incluyendo toda la cabeceraTCP/IP. Sin embargo, con un acceso de alta velocidad, esto no debería ser mayor problema.

Este *codec* es soportado por la mayoría de compañías de VoIP, tales como proveedores de servicio y fabricantes de equipos.

1.4.3.2 UIT G.729

Este *codec* comprime la señal en períodos de 10 milisegundos. No puede transportar tonos como DTMF o fax.

G.729 se usa principalmente en aplicaciones VoIP por su poca tasa de bits (8 kbps). Existen extensiones de la norma que permiten tasas de 6.4 y 11.8 kbps para peor y mejor calidad de voz, respectivamente. Idealmente presenta un MOS de 3.8.

El uso de aplicaciones usando este *codec* requiere una licencia. Sin embargo existen implementaciones gratuitas para uso no comercial.

1.4.3.3 GSM (RPE-LTP)

Este *codec* se llama oficialmente RPE-LTP (*Regular Pulse Excitation – Long Term Prediction*) pero se conoce mundialmente como GSM debido a que es el *codec* usado en el estándar GSM de comunicaciones móviles.

Tiene una tasa de bits de 13 kbps con un MOS ideal de 3.6 y realiza la codificación generando coeficientes representativos de un intervalo de tiempo determinado. Este intervalo normalmente es de 20 milisegundos de voz.

1.4.3.3 iLBC

iLBC (*Internet Low Bit-Rate Codec*) es un *codec* de voz de banda estrecha libre (se puede usar sin el pago de regalías).

La señal de voz es muestreada a 8 kHz., y el algoritmo usa una codificación predictiva lineal (LPC). Soporta dos tamaños de cuadro: 20 ms a 15.2 kbps y 30 ms a 13.33 kbps. La figura 1.8 muestra un estudio realizado por la empresa DynStat en el cual se comparan los protocolos iLBC, G.729 y G.723.1 en base a su robustez frente a la pérdida de paquetes. Para esto se midió el MOS conforme se iban perdiendo los paquetes. Al inicio de la prueba, iLBC presentó un MOS similar al G.729, y conforme se fueron perdiendo los paquetes presentó una mejor calidad.

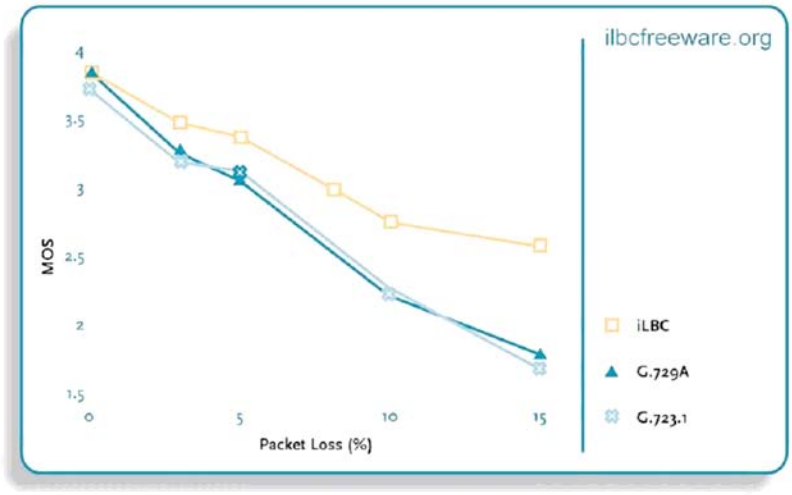


FIGURA 1.8: ROBUSTEZ FRENTE A PÉRDIDA DE PAQUETES

1.4.4 Hardware usado en los clientes

El hardware mencionado en este punto se refiere a los dispositivos usados por el usuario para comunicarse a través de la red de telefonía IP. Son básicamente dos tipos: Adaptadores analógicos y teléfonos IP propiamente dichos.

1.4.4.1 Adaptadores Analógicos:

Son dispositivos con una interfaz para conectar un teléfono analógico (*slot* para conector RJ-11) y otra interfaz para conectar a la red (*spot* para conector RJ-45). Básicamente su función es la de proveer señalización FXO a los teléfonos, es decir, se comporta como un dispositivo FXS. Se explicará brevemente estos dos términos:

FXO: *Foreign eXchange Office*, es la interfaz que se conecta a la red de Telefonía Básica (RTB, PSTN) o a una PBX y normalmente está presente en todos los teléfonos analógicos. Recibe la señalización dada por la FXS.

FXS: *Foreign eXchange Subscriber*, es la interfaz que se conecta directamente a un teléfono analógico y le brinda tono de timbrado y voltaje, entre otras cosas. En un escenario convencional (telefonía analógica), el FXS está en la central de conmutación, brindando señalización al dispositivo FXO (teléfono analógico).

Se tienen dos posibilidades para usar teléfonos analógicos en una red VoIP: Una es que el servidor de VoIP tenga una tarjeta con módulos FXS y la otra es tener en la red ciertos *gateways* que conviertan la señal analógica en datos IP. De esta forma, la PBX IP se comunica con los teléfonos analógicos a través de los *gateways* usando los protocolos de señalización mencionados anteriormente. Un ejemplo de estos *gateways* son los ATAs (*Analog Telephone Adapter*).

1.4.4.2 Teléfonos IP

Son dispositivos que soportan uno o varios protocolos de señalización. Entre las marcas más conocidas se tiene a Atcom, Cisco, Sipura (comprado por Cisco), etc. La gran mayoría soporta como mínimo el *codec* G.711, pudiendo soportar otros más. Adicionalmente pueden tener otras funcionalidades tales como supresión de silencios o conexión redundante a dos servidores.

1.5 Ventajas y desventajas de la Voz Sobre IP.

1.5.1 Principales ventajas de la VoIP

Una de las razones claves para el cambio de las redes de voz a datos, es una razón netamente económica, ya que las llamadas que se efectúen dentro de una misma red o una LAN son gratis gracias a que el costo de la llamada esta asociado al gasto de la manutención de la red por ser simplemente un dato que se desplaza en la red. También tenemos que contar que numerosas empresas han determinado que hoy en día cuesta varios pesos mover un teléfono, esto

no pasa para la telefonía IP ya que la red esta siempre y el mover el teléfono significa solamente cambiar de puerto del swicht al teléfono.

Otras ventajas importantes en la telefonía IP, se pueden apreciar en la siguiente lista:

- Una incrementada eficiencia para reducir tiempo y costos.
- La mejor dirección de información y control.
- Personalizados e integrados telecoms y sistemas IT para incrementar procesos en los negocios para ser estratégicamente competitivo.
- Integración sobre la intranet de la voz como un servicio más de la red, tal como otros servicios informáticos.
- Las redes IP son la red estándar universal para la Intranet y Extranets.
- Estándares H.323
- Interoperabilidad de diversos proveedores.
- Uso de las redes de datos existentes.
- Independencia de tecnologías de transporte.
- Menores costos que tecnologías alternativas (Voz sobre ATM, TDM, Frame Relay)

1.5.2 Principales desventajas de la VoIP

Los inconvenientes son:

- Puede haber un empeoramiento en la calidad de la voz.
- Hay que controlar el tráfico en la red local (LAN).
- Al ocupar un ancho de banda constante el número de operadores conectados puede estar limitado.

Si observamos con detenimiento las cantidades de ventajas con respecto a las desventajas e la voip son mas relevantes, es por esto que se puede decir que la voip es la comunicación de un futuro no muy lejano en donde las llamadas podrían ser hasta gratis.

CAPITULO II

PROPUESTA DE MEJORA AL SISTEMA IMPLEMENTADO (TRABAJO CON LOS ROUTERS)

2.1 Antecedentes

En el presente capitulo se realizara una descripción del esquema montado en un principio en el laboratorio, el cual fue tomado como base para la construcción de este tema de tesis y presento un punto de partida a la investigación que se deseaba realizar.

También se describirá el programa base utilizado, que es el SER, el que se utilizo en primera instancia en el servidor, y también el OPENSER, que fue el programa utilizado en los router que se utilizaron.

Es importante mencionar que el desarrollo de la tesis, fue apuntado al análisis de un sistema base, que se presenta en el capitulo, y el posterior traslado al router, analizando las capacidades de los mismos para soportar el esquema. El único objetivo del esquema anterior montado fue el probar si la comunicación de voz en distintos protocolos IP funcionaban y además sirvió para realizar pruebas anteriores a la homologación en los equipos utilizados, sabiendo así ciertos parámetros necesarios para la obtención de los router que se utilizaron y que se describen en el capitulo 3.

2.2 Esquema Basé.

En una primera instancia, solo se trabajo con un esquema básico que consistía en dos clientes de VoIP, uno con IPv4 y otro con IPv6, los cuales se comunicaban a trabes de una LAN corporativa, la cual estaba sobre un swicht Cisco Catalys 2950 que se encontraba en el sub-suelo del instituto de electricidad y electrónica, que es donde se desarrolla la tesis. El que controlaba el trafico de Voz entre los equipos era un servidor con plataforma Linux en donde se le instalo el software SER, el cual se describe en unos puntos mas adelante, y era el encargado de controlar el

trafico de los paquetes SIP y el que permitía la comunicación IP entre los dos clientes utilizados para las pruebas de comunicación echas al sistema implementado que se muestra en la figura 2.1.

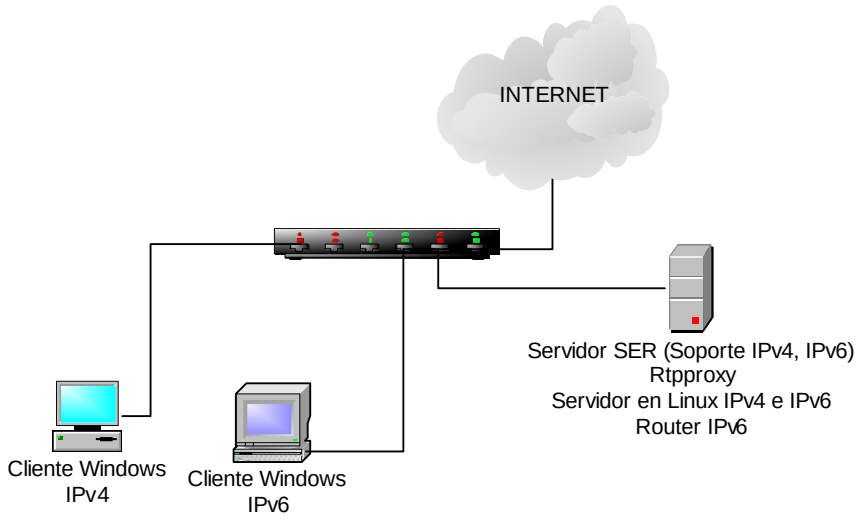


Figura 2.1: Esquema Basé del proyecto

Podemos observar claramente que el esquema de la figura 2.1, es un sistema tradicional de telefonía IP donde tenemos un servidor que controla todo dentro de la red, ahora lo que el trabajo de titilación persigue es analizar las potencialidades de los router, en particular aquellos que están basados sobre plataforma debían Linux, para así disminuir la cantidad de programas que se requieran en un servidos y lograr de esta forma eliminar ha este equipo de la red LAN y crear así un sistema mas compacto.

Cabe mencionar que por arquitectura de la red LAN, el swicht que se muestra en la figura 2.1 no se puede eliminar de la red montada para las pruebas en el laboratorio, ya que es el distribuidor de la Internet a los computadores de la sala de comunicaciones modernas de Instituto de electricidad y electrónica y del instituto mismo, por lo cual no se elimina pero se debe tener en cuenta que el router puede estar por si solo en una red LAN interna, sin necesidad de un swicht antes de él para prestar los servicios de telefonía e Internet, solo se necesitaría un MODEM.

De este esquema se realizaron pruebas de comunicación resultando exitosas tanto en comunicación de equipos con IPv4 – Ipv4 como con equipos IPv4 – Ipv6, lo que nos llevo de inmediato a pasar a homologar estos servicios a los router en cuestión escogiéndose los modelos

LINKSYS WRT54G y el NETGEAR WGT634U, por los antecedentes y motivos que se describen en detalle en el capitulo III.

Es importante mencionar que no se explica en detalle ni la configuración de este servido ni tampoco las pruebas que se el desarrollaron por los antecedentes antes expuestos y se sale de entre los objetivos planteados en el tema de tesis, ahora solo se puede decir que las pruebas realizadas a este esquema también se le realizaron a los router y se expresaran en detalle en el capitulo V de resultado y pruebas, dejando en evidencia el correcto funcionamiento de los equipos y del sistema montado.

2.3 Esquema Actual.

Ahora, en este punto, se a configurado el nuevo esquema de red, que consiste en un router que se le han mejorado sus capacidades cambiándole su sistema operativo (frimware) y sobre este se le han cargado servicios como es el openser, aparte de los servicios básicos que posee un router normal. En la figura 2.2 se muestra el esquema que se monto en el laboratorio.

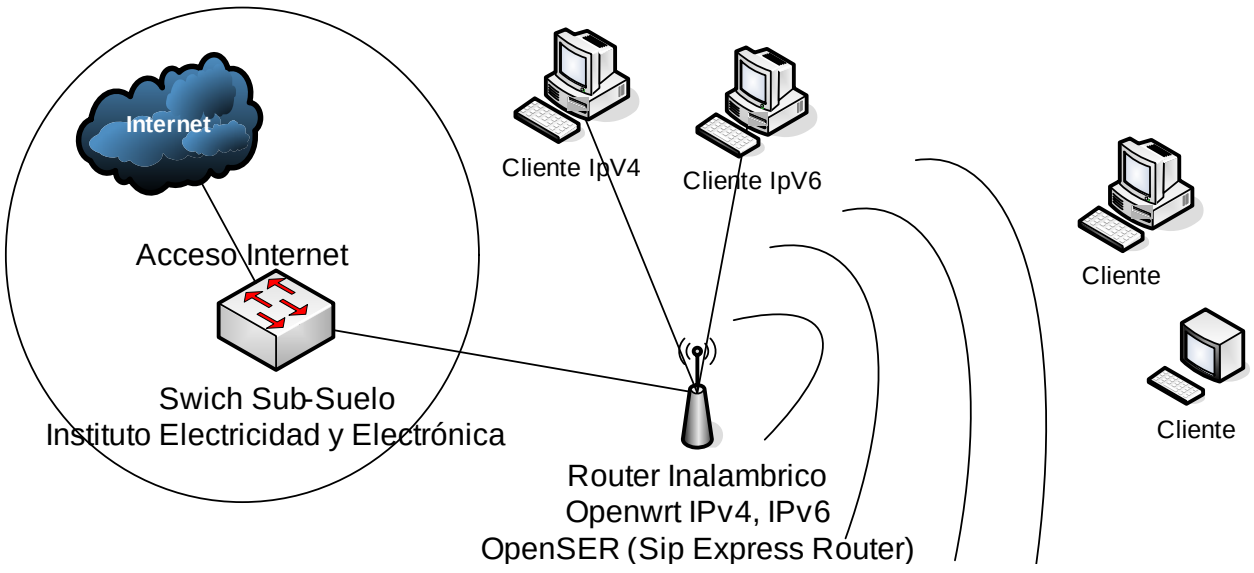


Figura 2.2: Esquema montado en el laboratorio

Si realizamos un análisis a la figura 2.2 observamos que el swicht Catalys que se encuentra en la figura no se ha quitado de la arquitectura anterior (Ver figura 2.1) esto se debe a que este swicht es el que nos proporciona conectividad Internet, es por esto que no se ha quitado de la arquitectura actual, ahora si llegáramos a contar con un MODEM, ya este swicht es innecesario y se puede no utilizar. De echo, el sistema se desarrollo pensado que el router maneja prácticamente todo dentro de la red, pero por la arquitectura de prueba es imposible quitar el swicht de la conexión.

Cada uno de los router fue configurado con IP statica para las respectivas puertas WAN de los routers utilizados, ya que la configuración de la red Lan donde se trabajo estaba configurada de esta forma. Pero los routers también se pueden configurar en forma PPPOE, PPPOA, DHCP, como uno desee y según las necesidades del usuario. La configuración del router Netgear se puede ver en la figura 2.4, en donde la IP asignada a este router fue 200.2.114.212; Mascara 255.255.255.192 y puerta de enlace 200.2.114.193; los DNS fueron 200.2.114.215 y 146.83.216.4. Para el router Linksys la IP fue 200.2.114.216 y los parámetros de mascara y puerta de enlace como también los DNS fueron los mismo del Linksys (ver figura 2.3).

Figura 2.3: Configuración WAN del Router Linksys

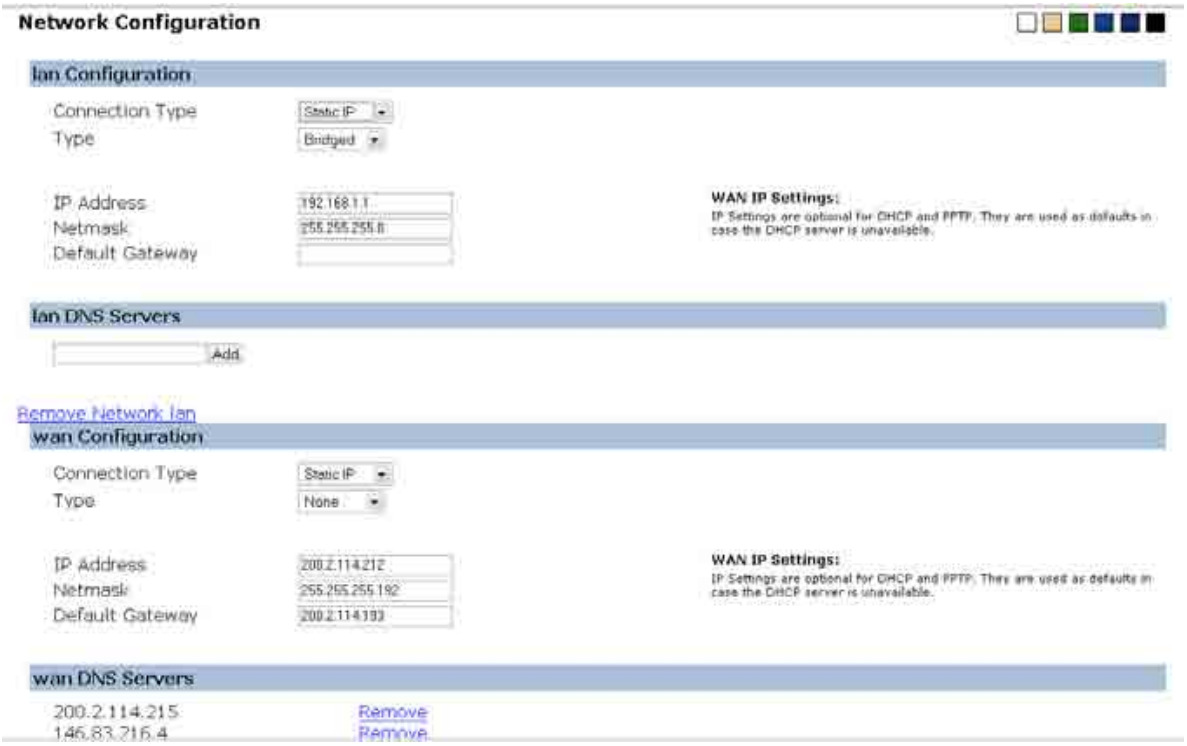


Figura 2.4: Configuración WAN de router Netgear

Para la configuración LAN, como se deseaba tener un control de los equipos conectados a la Red Lan utilizada, se configuraron con IP statica pero sin dejar de lado la posibilidad de trabajar con un servidor DHCP que viene integrado dentro del frimware instalado en cada router. Para la configuración Lan se utilizaron las IP no validas 192.168.1.X, la puerta de enlace para cada router 192.168.1.1 y la mascara por defecto 255.255.255.0; utilizando esta configuración para el router linksys como para el router netgear. En las figuras 2.3 y 2.4 se pueden observar las configuraciones de la red Lan de los routers.

La configuración wireless de los router no fue necesaria ya que no era importante probar los equipos utilizando la red inalámbrica ya que si funcionaban con la red Lan cablead ya era suficiente para probar que el sistema funciona. Pero es importante destacar que la configuración misma de las tarjetas inalámbricas de cada router depende exclusivamente del tipo de frimware que se utilice, ya que la versión white_russian_rc6 instalada en el router linksys, viene la configuración por defecto de la red inalámbrica, pero la versión Kamikaze, instalada al router

Netgear, hay que configurar la re inalámbrica de forma manual a trabes de línea de comandos con la conexión SSH que tienen los router (Para mas detalles ver Capitulo IV).

Como objetivo de la tesis, estos router deben tener soporte para IPv6, para lograr esto se le cargaron strip y se instalaron unos paquetes propios del frimwares que se describirá en el punto 2.4 de este capitulo.

2.4 Configuración Protocolo Ipv6 en los Routers.

Para la configuración del protocolo ipv6 en los routers, se tuvieron que instalar paquetes especiales para el soporto ipv6, como lo son el radvd, la iptable y kmod, cada uno de ellos nos da soporte para que el router pueda funcionar bajo Ipv6 y después poderle configurar la dirección ip que se desea colocarle a este router. Es importante destacar que la dirección Ipv6 configurada en los router funcionan creando un túnel montado en protocolo ipv4, en pocas palabras los datagramas ipv6 de 128bit con encapsulados en datagramas ipv4 de 32 bit cada uno. El detalle de cómo encapsular los datagramas lo podemos leer en el apartado 2.4.1 del presente capitulo.

Para la configuración de los routers se siguieron los siguientes pasos, que se repitieron tanto para el router linksys como para el router netgear. (La explicación de este procedimiento se dará a conocer de forma general, ya que para los dos router fue exactamente lo mismo). Antes de describir los pasos que se llevaron acabo para la instalación de soporte IPv6 en el router, es necesario saber que se requieren de ciertos módulos instalados en el Kernel de frimware para que funcione, los cuales son:

- Modulo IPv6 del Kernel, siempre debe estar instalado, por ser la base del programa.
- Software de enrutamiento IPv6, siempre debe ser instalado ya que nos permite el enrutamiento IPv6
- Módulos del núcleo IPv6tables, de forma opcional si se requiere de un firewall IPv6

- Herramienta IPv6tables, de forma opcional ya que sirve para la configuración del servidor de seguridad IPv6.

Todos estos módulos fueron instalados en los router para que pueda tener soporte IPv6, utilizando las líneas de comando ejecutados como usuario root, como se describe a continuación:

- *Instalación del IPv6 del Kernel:*

  ipkg install kmod-ipv6

- *Instalación del router de enrutamiento*

  ipkg install radvd

  ipkg install ip

(Aquí se necesito instalar el radvd, que actúa como demonio, y el IP que configura la dirección IP por defecto.)

- *Módulos del núcleo IPv6tables*

  ipkg install kmod-ip6tables

- *Módulos del núcleo IPv6tables*

  ipkg install ip6tables

Una ves terminada la instalación de estos módulos en el frimware, con el comando *ifconfig,* escrito en la consola, se puede comprobar si la instalación de los módulos quedo correctamente, pues aparece la dirección ipv6 nativa en las puestas del router, con el rotulo de *inet6 addr*, y es totalmente identificable puesto que posee una numeración distinta a la de la versión IPv4. Es importante mencionar que las direcciones en IPv4 deben ser de IP fijas para que se pueda generar la dirección Ipv6. En la figura 2.5 se puede observar esta dirección con mayor claridad. (Esta es una fotografía del router linksys, y corresponde a la dirección destacada).

```
br0       Link encap:Ethernet  HWaddr 00:12:17:30:DA:A9
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::212:17ff:fe30:daa9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43903 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33145 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6258471 (5.9 MiB)  TX bytes:8717640 (8.3 MiB)

eth0      Link encap:Ethernet  HWaddr 00:12:17:30:DA:A9
          inet6 addr: fe80::212:17ff:fe30:daa9/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:695884 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76603 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:81072655 (77.3 MiB)  TX bytes:16061285 (15.3 MiB)
          Interrupt:5

eth1      Link encap:Ethernet  HWaddr 00:12:17:30:DA:AB
          inet6 addr: fe80::212:17ff:fe30:daab/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:56
          TX packets:0 errors:5 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:95 (95.0 B)  TX bytes:0 (0.0 B)
          Interrupt:4 Base address:0x1000
```

Figura 2.5: despliegue del comando ifconfig.

Después de instalar estos módulos, se deben configurar el demonio radvd para que acepte direcciones ipv6 modificando sus parámetros prefix, el contenido del fichero radvd.conf que se encuentra en la carpeta etc/, debe estar configurado como lo muestra la figura 2.6.

```
root@Linksys:/etc# cat radvd.conf
# For more examples, see the radvd documentation.

interface br0
{
#       AdvSendAdvert off;
        AdvSendAdvert on;


#
# Disable Mobile IPv6 support
#
        AdvHomeAgentFlag off;

#
# example of a standard prefix
#
#       prefix fec0:0:0:1::/64
prefix 2001:1310:a111:1211::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        };

};
root@Linksys:/etc#
```

Figura 2.6: configuración del radvd.conf

Como se muestra en la figura 2.6, se debe configurar el prefijo de la dirección IPv6 que se utilizara y dejar deshabilitado el prefijo de la dirección IPv6 nativa que tiene por defecto configurada, teniendo en cuanta que se debe poner especial cuidad en declara bien la puerta en que deseamos que tenga este prefijo de dirección IPv6, para que la configuración después funcione.

Luego de esto se deben crear dos script en la carpeta etc/init.d, los cuales nos servirán para activar la dirección IPv6 y desactivar la dirección IPv6. El primero es activar la dirección IPv6, que como muestra la figura 2.7, consiste en declarar la dirección que se desea cargarla al equipo y la interfaz en la que debe quedar configurada dicha dirección junto con su dirección IP del router que en este caso, y en el del otro router, se le coloca la por defecto, y por supuesto activar esto para el radvd. Luego la figura 2.8 nos muestra la forma de desactivar esta opción, que es simplemente deteniendo el radvd, quedando a simple vista que el demonio radvd es el que nos controla las direcciones IPv6 que quisiéramos cargarle al router en cuestión, o de cualquier maquina que deseemos cargarle el soporte IPv6, ya que cuando se montaron estos script en el pc que tenia Linux y soporte IPv6, también se realizaron procedimientos similares.

Figura 2.7: Script IPv6_active

Figura 2.8: Script IPv6_deactive

Luego de haberle echo estas modificaciones, solo quedaba ejecutar el script que se creo para ejecutar la dirección IPv6 (ver figura 2.9), con esto probábamos que funcionaba correctamente, y luego se realizaba un ifconfig y aparecía lo que se muestra en la figura 2.10.

```
root@Linksys:/etc/init.d# ./ipv6_active
Syntax: ./ipv6_active [command]

Available commands:
        start   Start the service
        stop    Stop the service
        restart Restart the service
        reload  Reload configuration files (or restart if that fails)
        enable  Enable service autostart
        disable Disable service autostart

root@Linksys:/etc/init.d#
```

Figura 2.9: activación del script IPv6_active

```
root@Linksys:/etc/init.d# ifconfig
br0       Link encap:Ethernet  HWaddr 00:12:17:30:DA:A9
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:1310:a111:1211::1/128 Scope:Global
          inet6 addr: fe80::212:17ff:fe30:daa9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:56292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9141471 (8.7 MiB)  TX bytes:10164159 (9.6 MiB)

eth0      Link encap:Ethernet  HWaddr 00:12:17:30:DA:A9
          inet6 addr: fe80::212:17ff:fe30:daa9/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:738729 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97721 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:87945016 (83.8 MiB)  TX bytes:20703943 (19.7 MiB)
          Interrupt:5

eth1      Link encap:Ethernet  HWaddr 00:12:17:30:DA:AB
          inet6 addr: fe80::212:17ff:fe30:daab/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:56
          TX packets:0 errors:5 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:95 (95.0 B)  TX bytes:0 (0.0 B)
          Interrupt:4 Base address:0x1000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

vlan0     Link encap:Ethernet  HWaddr 00:12:17:30:DA:A9
          inet6 addr: fe80::212:17ff:fe30:daa9/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:56277 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9366399 (8.9 MiB)  TX bytes:10333199 (9.8 MiB)
```

Figura 2.10: Despliegue del comando ifconfig con Dir IPv6 activada

En la figura 2.10, se resalta la dirección IPv6 que estamos utilizando la que corresponde ha 2001:1310:a111:1211::1/128 y que esta configurada en la puerta br0, que corresponde a las puestas Lan del router utilizado, si se observa en las otras puertas no esta configurado las direcciones IPv6, si se deseara se tendrían que modificar el radvd.conf para las puertas que se desean configurar con una dirección IPv6 deseada y los script para cargar las direcciones activando el radvd.

Con esta configuración lista ya se podía trabajar con soporte para dirección IPv6, pero se requería de un equipo que ojala tuviera Windows xp instalado que tuviese soporte IPv6, para ello a uno de los PC de prueba se le instalo el modulo para Windows de soporte IPv6, lo que resulto muy fácil, por que es tan simple como ejecutando en CMD *"ipv6 install"* y listo ya quedo instalado el soporte para Windows IPv6, donde se puede ver que aparece un TCP/ipv6 en las propiedades de red. (Ver figura 2.11)

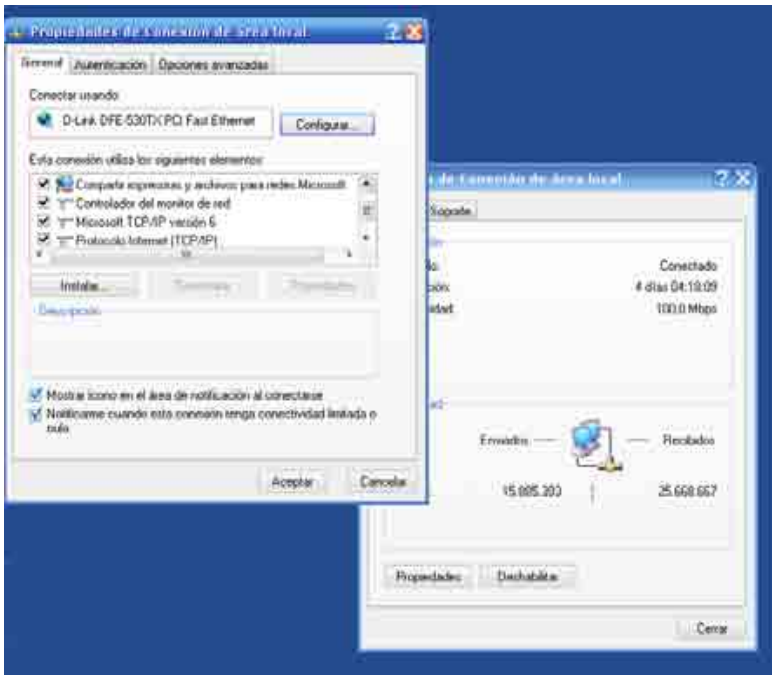


Figura 2.11: Propiedades de Red con Soporte IPv6 del PC cliente

2.4.1 Túneles de IPv6 sobre IPv4

Un túnel de IPv6 sobre IPv4 consiste en encapsular un datagrama IPv6 en un datagarama IPv4. En la anterior Figura 2.12 se resume esta técnica. En dicho ejemplo si la máquina “A” (IPv6) desea enviar un datagrama IPv6 a la máquina “E” (IPv6), el router “B” encapsula dicho datagrama IPv6 en un datagrama IPv4 para enviárselo a “C” (IPv4). Se resalta que un inconveniente de esta solución es que los extremos de cualquier túnel deben conocerse previamente. Por consiguiente, en este ejemplo, los routers “B” y “D” tienen que conocer la dirección IPv4 del otro router con antelación. En este contexto, el primer router “B” cambia las direcciones de origen y destino IPv4 de la cabecera de información de control del datagrama IPv4. Ahora, el origen y destino de dicho datagrama IPv4 serán “B” y “D” respectivamente. El router “B”, por ser el extremo transmisor en el túnel, es decir, por realizar el encapsulado del datagrama IPv6 y el router “D” por ser el extremo receptor del túnel, es decir por llevar a cabo, a su vez el desencapsulado final del datagrama IPv6. El resultado es que, finalmente, llega a la máquina destinataria “E” el datagrama IPv6 original tal y como salió de origen (“A”) sin la pérdida de ninguna información de control. Obviamente, el mismo procedimiento18 se repite en sentido contrario en las respuestas de la máquina “E” a la máquina “A”.

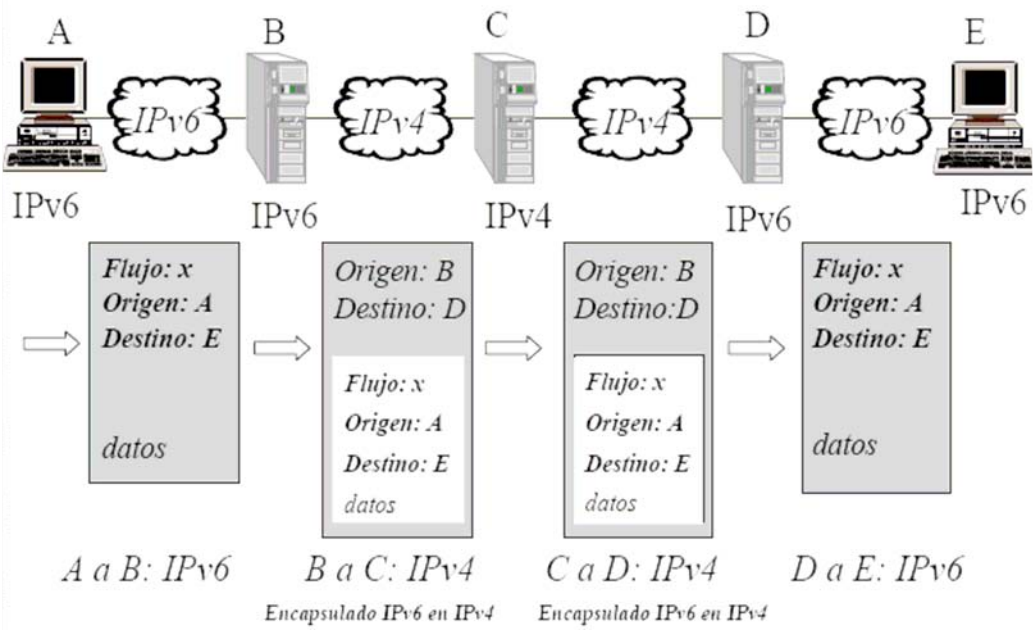


Figura 2.12: Túnel Ipv6 sobre IPv4

En la siguiente Figura 2.13 se muestra la arquitectura de protocolos de las máquinas del citado ejemplo. Es importante resaltar que, en dicho ejemplo, se ha realizado un túnel para dos redes IPv6 (a las cuales se conectan “A” y “E” respectivamente), es decir, dicho túnel permite conectar a cualquier máquina de una red IPv6 (por ejemplo, “A”) con cualquier otra máquina de la otra red IPv6 (por ejemplo, “E”). Esta solución tiene un inconveniente y es que, mientras esté establecido el túnel, no se puede comunicar ni “A” ni “E” con ninguna otra máquina conectada a una red IPv4.

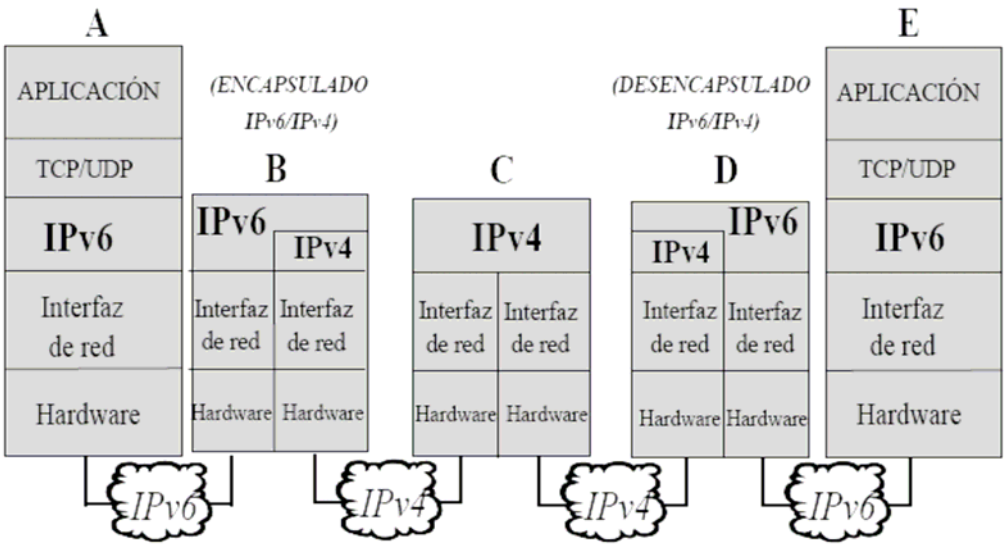


Figura 2.13: Arquitectura de comunicaciones del ejemplo

Según muestra la siguiente Figura 2.14, para poder establecer un túnel de IPv6 sobre IPv4, es decir, encapsular IPv6 sobre IPv4, es necesario insertar un 41 en binario (00101001) en el campo Protocolo de la primera cabecera de información de control (IPv4) que es la que establece el correspondiente túnel.

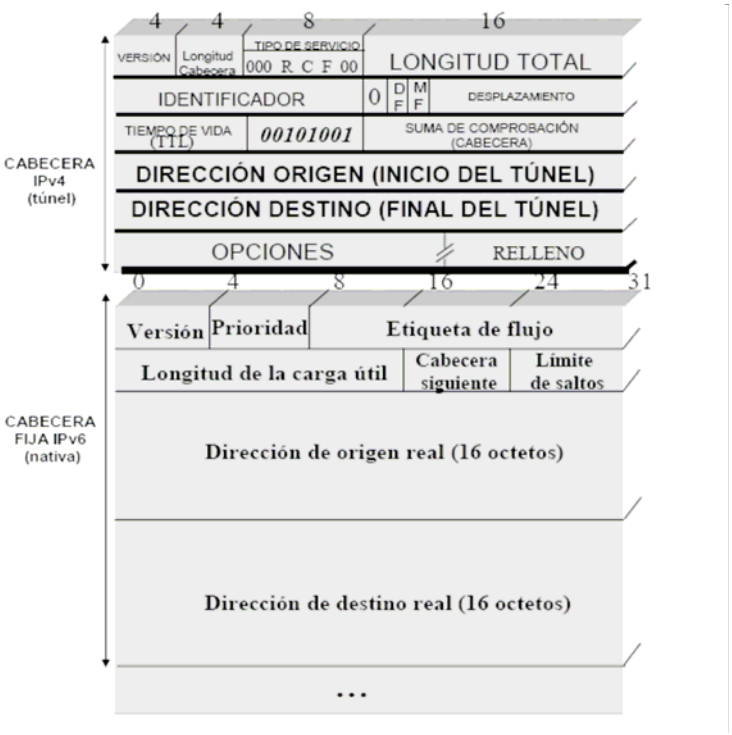


Figura 2.14: Encapsulación de IPv6 sobre IPv4.

A continuación se explicara en que consiste el programa Openser, que se utilizo en los router, y cual fue la metodología para su instalación como también su forma de operación.

2.5 Openser (open Sip Express Router)

2.5.1 ¿Que es Openser?

Para poder hablar a ciencia cierta del openser, debemos pasar primero por hablar del SER que sus siglas en ingles significan SIP EXPRESS ROUTER, que en resumidas cuentas es uno de los servidores Proxy VoiP SIP mas utilizados por que cuenta con licencia abierta para la señalización de voz, extremadamente configurable que permite crear varias políticas de enrutamiento y de admisión, así como la configuración de servicios nuevos y personalizados (soporte SMS, mensajería basada en SIP, etc.) también incluye soporte para actuar como servidor de registro, Proxy (stateless y statefull) y de redirección. SER fue creado por la organización iptel.org, portal que promueve las tecnologías de VoIP y que fue inicializada por el instituto de

investigación alemán Fraunhofer Fokus. Funciona bajo un sistema operativo Linux, soporta 150 llamadas por segundo y esta programado en lenguaje C.

Este Proxy esta programado de forma modular. Los módulos se cargan dentro del núcleo del SER en el momento de arrancar por medio de un archivo de texto de configuración llamado *"ser.cfg"*. Esta propiedad hace que el SER sea configurable por el usuario cargando los módulos que le interesan e incluso crear sus propios módulos siguiendo unas pautas marcadas por iptel.org. Entre los módulos desarrollados por iptel.org cabe destacar:

- ✓ **Auth y auth_db:** contienen las funciones necesarias para la autentificación con la base de datos.

- ✓ **Enum:** (Electronic NUMber/tElephone NUmber Mapping). Implementa las funciones necesarias para transformar un número de teléfono internacional en una consulta a una base de datos ENUM de un servidor DNS.

- ✓ **Msilo:** este módulo proporciona la opción de poder enviar mensajes a los usuarios del SER que se encuentren offline. Cuando un usuario offline se conecta, se le envían todos los mensajes almacenados.

- ✓ **Nathelper:** este módulo incorpora la ayuda necesaria para poder atravesar los NAT trasversales.

- ✓ **Pa:** este módulo implemente un servidor con estado de presencia. Es decir, el servidor avisa cuando el estado de algún usuario cambia.

- ✓ **Permissions:** este módulo es usado para determinar si una llamada tiene permiso para establecerse.

- ✓ **Pdt:** este módulo traduce los códigos numéricos a dominios y los actualiza respecto al R-URI.

- ✓ **Registrar:** el módulo contiene el proceso lógico para los mensajes *REGISTER*.

- ✓ **Sms:** este módulo hace posible la comunicación entre SIP y la red de GSM. La comunicación es posible mediante SIP a SMS y viceversa.

- ✓ **Transaction:** implementa la lógica necesaria para gestionar las transacciones SIP.

Además ofrece la posibilidad de gestionar los usuarios de la base de datos del SER a través de la consola gracias al comando "serctl". Esta herramienta contiene las opciones de crear, modificar o eliminar usuarios autorizados a utilizar el SER o a mostrar que usuarios se encuentran online, entre otras opciones.

Aparte del SER desarrollado por iptel.org, existe un proyecto paralelo llamado OPENSER. Este proyecto esta dirigido por 3 de los programadores del SER y consiste en desarrollar nuevos módulos para este servidor Proxy. Para un desarrollo más rápido se cuenta con la aportación desinteresada de la comunidad SIP. Si se crean nuevos módulos interesantes, estos se acaban integrando en el SER. Es este el que se instala directamente en los router, gracias a que el frimware OPENWRT lo trae dentro de sus paquetes opcionales de trabajo, lo que lo hace sumamente simple de instalar y configurar dentro de este sistema operativo.

Una de las ventajas importantes del openser (o del SER), es que se puede hacer correr dentro de u PC con recursos limitados, y como los routers son de recursos limitados entonces nos permitía un mucho mejor trabajo dentro del router a utilizar, aparte de la opción de control que tiene, que como en el caso de ser era *serctl,* en el openser es *openserctl.*

2.5.2 Instalación y configuración del Openser.

En la instalación del openser, se realizaron de forma similar en los dos routers, ya que tenían el mismo frimware pero con versiones distintas, el router netgear tiene la versión

Kamikaze y el router linksys la versión Write_russian 6.0, es por esto que se realizaron de formas distintas, pero en el fondo los procedimientos son exactamente los mismos.

Para el caso del router linksys, se procedió a buscar el paquete en la opción *"system"* del panel de categoría, y luego seleccionar la opción *"Installed Software"* y luego en la lista que aparece buscar el paquete *"openser"*, hacer clic y listo, el openser esta listo para ser utilizado. Es importante mencionar que como las limitaciones del routers son muchas, por la cantidad de memoria que se cuenta (sale descrito en el capitulo III), es importante testear cuanta memoria nos queda para seguir instalando programas, puesto que el frimware trae como un error, que al momento de saturarse la memoria ROM ya no se pueden instalar ni desinstalar programas mandando un error y cuya única solución es volver a instalar el frimware o a través de modo de comandos liberar la memoria eliminado paquetes no importantes con el comando *"IPKG"*. La figura 2.15, nos muestra la lista de programas que se muestra al momento de la instalación.

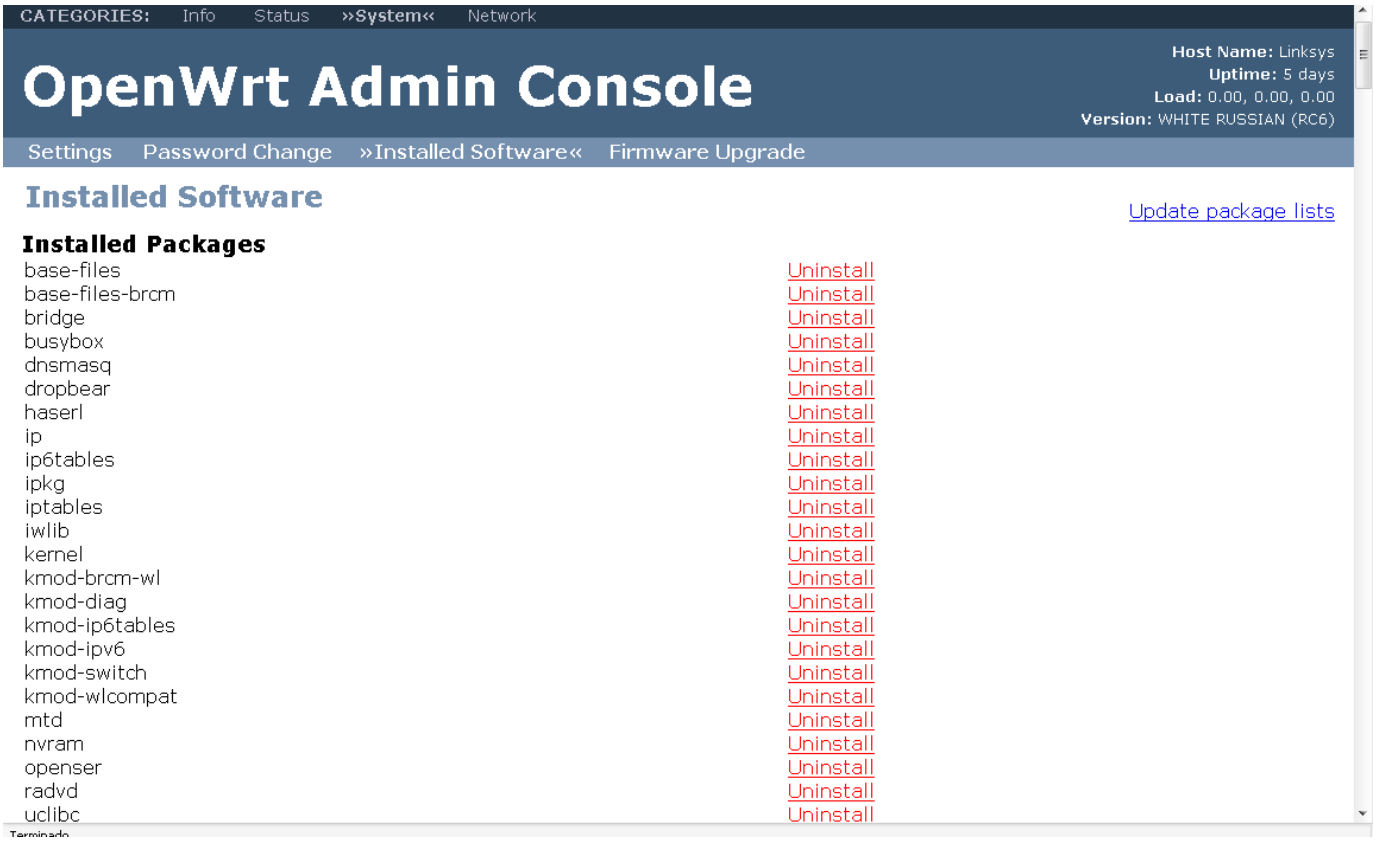


Figura 2.15: Lista de programas instalados en router linksys.

Para el caso del router Netgear, como era la versión Kamikaze, instale el openser con el modo de comandos, ejecutando el comando *"ipkg install openser"*, como lo muestra la figura 2.16. Se utilizo este método solo para realizarlo como una prueba, pero se podía realizar de el otro modo a través de la interfaz WEB que se le instalo el frimware versión kamikaze, ya que esta versión del openwrt no cuenta con una interfaz WEB por defecto, como lo es para el caso del write_russian 6.0.

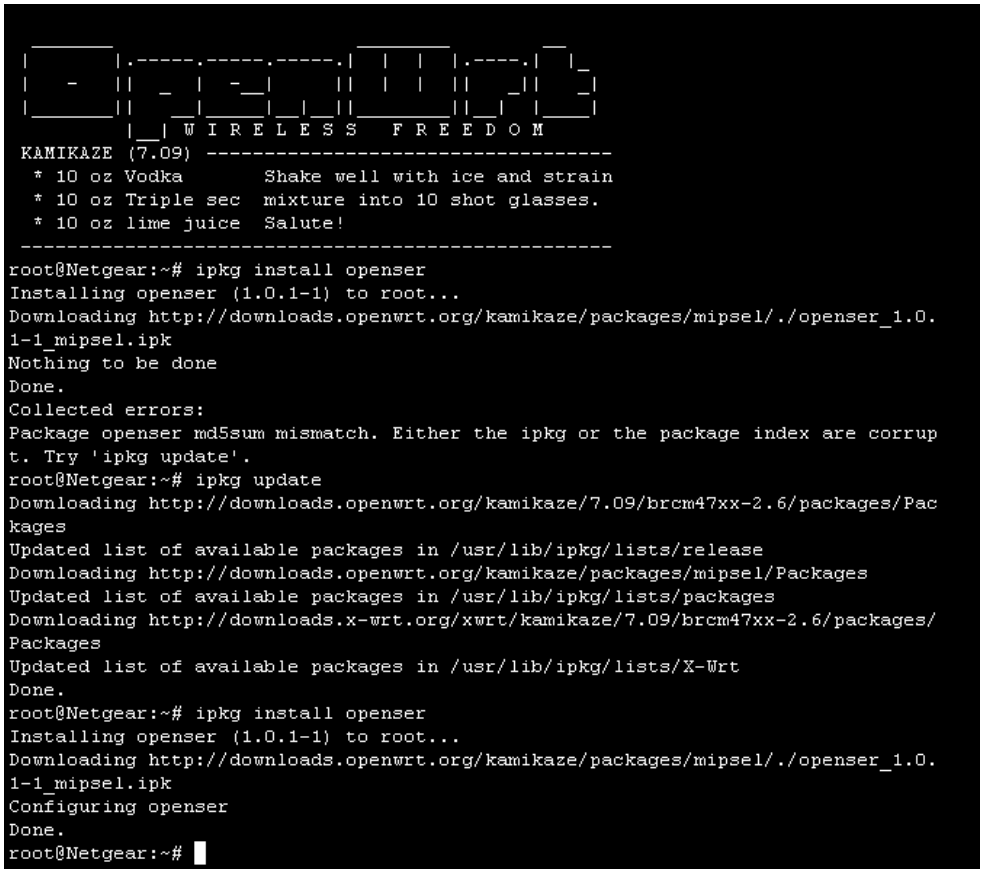


Figura 2.16: Instalación Openser en Netgear

Ahora, si hablamos de la configuración del Openser, se puede hablar perfectamente que en los dos routes se utilizo exactamente la misma configuración, de hecho no se tubo que configurar absolutamente nada, una ves instalado se podía utilizar de inmediato el programa ya que se utilizo en su forma mas basita, por defecto, que nos permitía conectar cualquier cantidad de usuarios sin necesidad de tenerlos registrados en alguna base de datos y sin ninguna contraseña, como el objetivo de la tesis es probar las capacidades de los routers, y probar si funciona el esquema señalado en la figura 2.2, no nos intereso configurar la base de datos MSQL

que trae el Openser para que pueda funcionar de forma normal, necesitando identificar un nombre de usuario y contraseña. Ahora el problema que se podría presentar son, nuevamente, las capacidades de almacenamiento que tenga el router, eso queda resuelto colocando un disco externo al router para poder soportar una cantidad mayor de información. Aunque esto se puede hacer con el router netgear, pero no con el router linksys, las pruebas de esta teoría no se realizaron, pero si se esta seguro que se le puede incorporar un dispositivo de almacenamiento masivo al router netgear por su puerto USB que cuenta y poder acceder a el a través de la consola como usuario *root*.

Para hacer correr el Programa, se debe hacer uso del comando *"openserctl Start"*, con este comando se puede hacer partir sin problemas el router, si deseamos monitorear a los usuarios se puede utilizar el comando *"openserctl moni"* y para detener el programa simplemente se coloca *"openserctl stop"*. Ahora si deseamos información de los usuarios (clientes), debemos utilizar el comando *"openserctl alias show"*, así podemos ver la información de los usuarios conectados.

En la figura 2.17, muestra la ejecución del comando para hacer partir el openser y el PID que entrega al momento de iniciado.

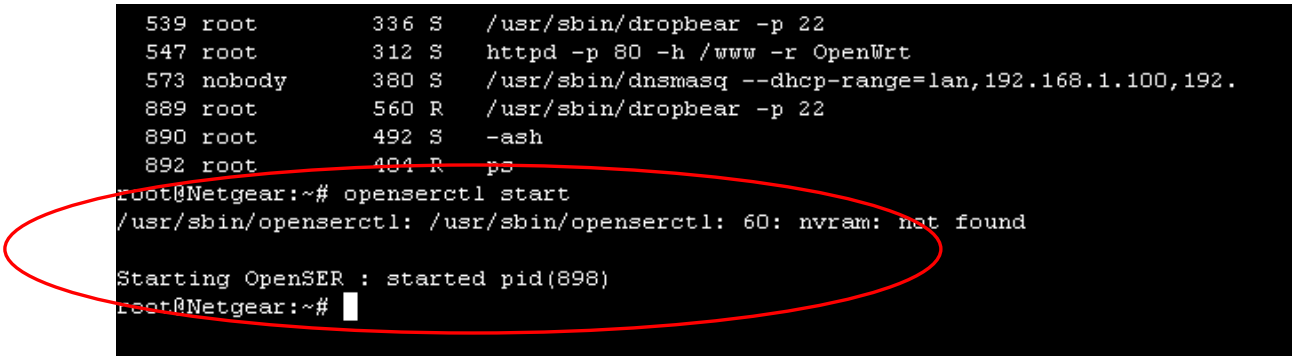


Figura 2.17: Inicialización OPENSER

Ahora, como el trabajo de titilación comprende también el trabajo con Protocolo IPv6, para iniciar el openser con protocolo IPv6 hay que indicarle la IPv6 que debe iniciarse el

programa, ya que la inicialización con el método de la figura 2.17 es solo cuando se desea trabajar con el protocolo Ipv4. La forma de indicarle al IPv6 es con el comando *"openser –l [2001:1310:a111:1211::1]"* con eso el openser queda escuchando direcciones IPv6 solamente, ahora si quisiéramos que escuchara Protocolos IPv6 e IPv4, entonces se debe utilizar el mismo comando pero asignándole las direcciones IP que nosotros necesitamos que esculle. En la figura 2.18 podemos ver ya inicializado el openser con IPv6, así se pueden realizar llamadas en el protocolo IPv6, ahora en la figura 2.19 comprobamos desplegando la lista de procesos que el openser esta corriendo con soporte exclusivamente para IPv6.

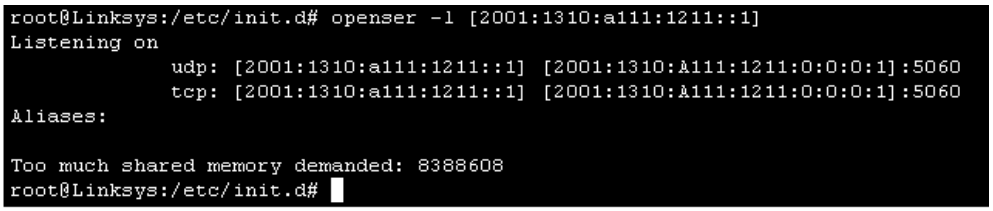


Figura 2.18: Inicialización con soporte IPv6

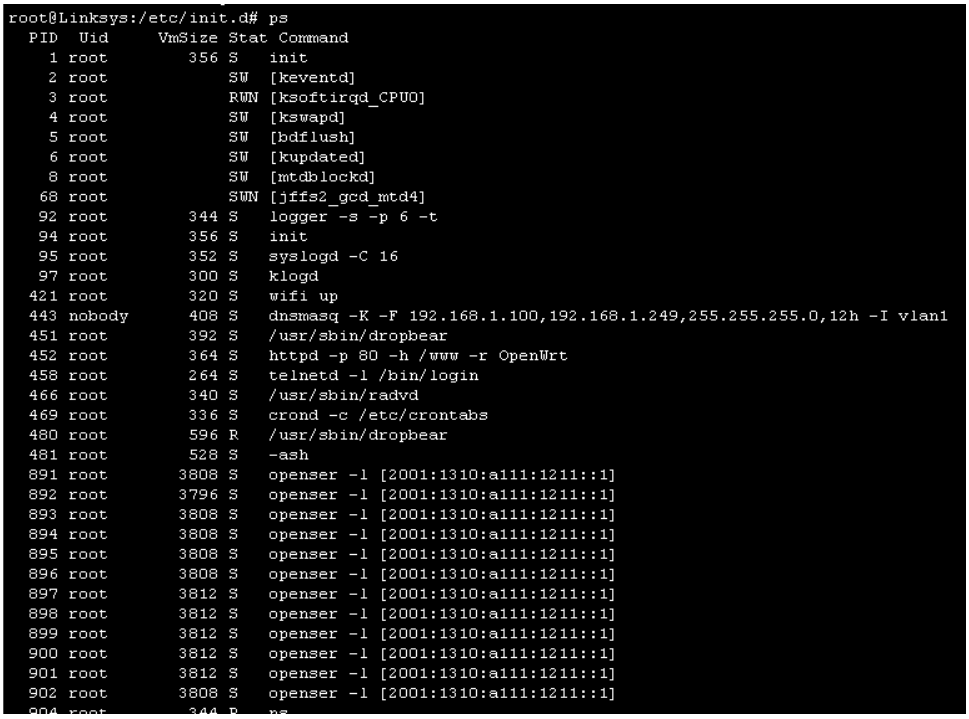


Figura 2.19: Lista de procesos

Es importante mencionar que el soporte para IPv6 y la dirección IPv6 que se le declarara al openser debe estar cargada y corriendo para que este pueda funcionar con el soporte

IPv6, también es importante que ya no se hará arrancar el openser de la forma tradicional, si no que solamente como se expresa en la figura 2.18 y asignándole todas las direcciones IP que se requiere que el programa escuche al momento de realizar las llamadas entre los clientes de prueba. En la figura 2.20 muestra la inicialización del openser con soporte para el protocolo IPv4 e IPv6, asignándole las IP que tiene el router, tanto para el protocolo IPv4 como para el Protocolo IPv6.

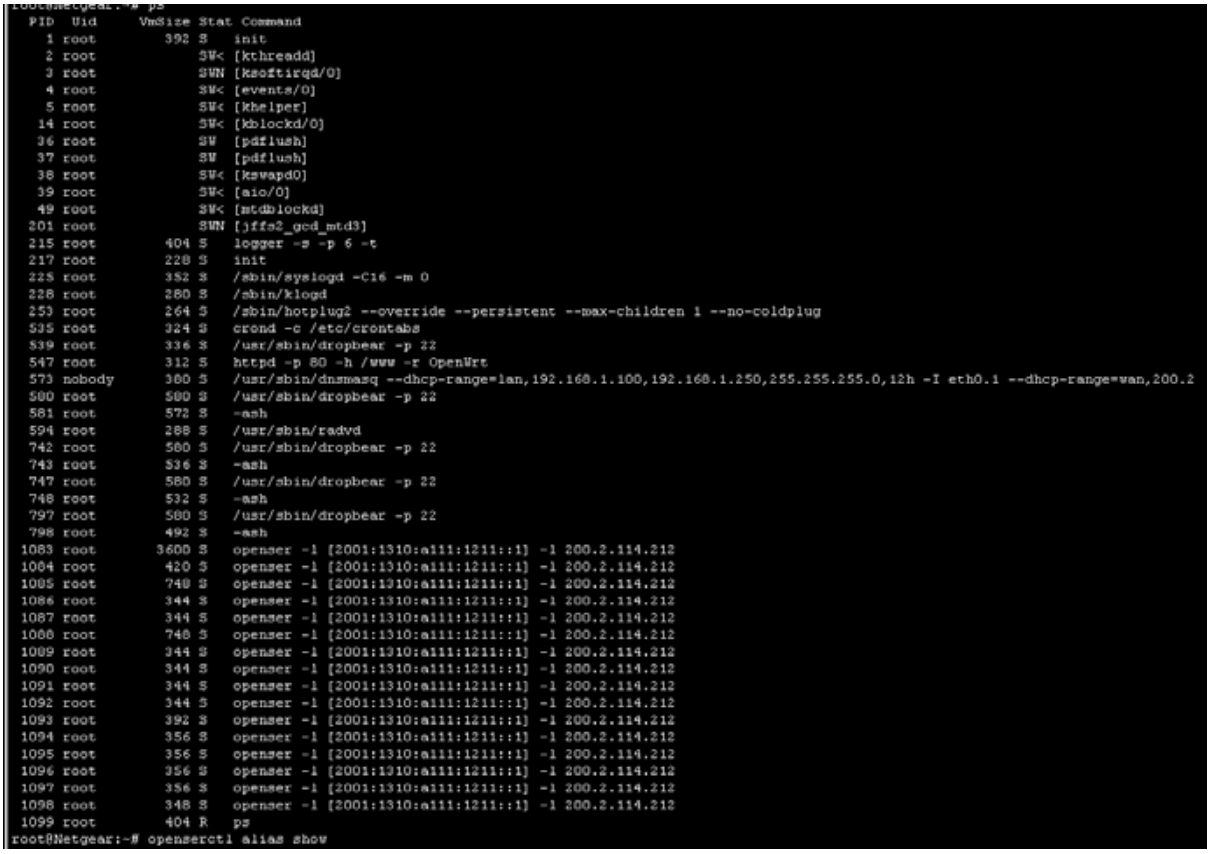


Figura 2.20: Tabla de procesos

Para lograr lo que muestra la figura 2.20, se deben asignar al openser todas las direcciones que se desean escuchar, como es en este caso, la dirección IPv4 y la IPv6 con el comando *"openser –l [direccion_IPv6] –l direcci0n_ipv4"*, con esto el programa estará escuchando las dos direcciones asignadas como lo muestra la figura 2.21

```
 1080 root        404 R   ps
root@Netgear:~# openser -l [2001:1310:a111:1211::1] -l 200.2.114.212
Listening on
             udp: [2001:1310:a111:1211::1] [2001:1310:A111:1211:0:0:0:1]:5060
             udp: 200.2.114.212 [200.2.114.212]:5060
             tcp: [2001:1310:a111:1211::1] [2001:1310:A111:1211:0:0:0:1]:5060
             tcp: 200.2.114.212 [200.2.114.212]:5060
Aliases:
```

Figura 2.21: Inicialización con soporte mixto

A continuación en el capitulo III, se explicaran los materiales utilizados y en especial las características técnicas de los routers utilizados.

CAPITULO III
MATERIALES Y METODOS

3.1 Antecedentes

En el presente capitulo esta compuesto por una descripción de los materiales utilizados, que en este caso corresponden a dos router adquiridos en mercado, uno de ellos es el Linksys modelo WRT54G v2.0 y el otro router utilizado es un Netgear modelo WGT634U. Además de una descripción de los softphone utilizados para las pruebas de voz, para las distintas versiones de IP que se utilizaron.

A continuación se darán a conocer las características técnicas y el por que se escogieron en particular estos dos router inalámbricos para el desarrollo del presente trabajo de tesis.

3.2 Características de los routers utilizados

3.2.1 Router Linksys

La figura 3.1 nos muestra la forma física del router linksys modelo WRT54G que se utilizó. Este router tiene características técnicas bastante especiales, que fue lo que determino su utilización. Este modelo de router presenta una gran familia de routers, los cuales podemos apreciar junto con sus características de fábrica en la tabla 3.1

Figura 3.1: Router linksys WRT54G v2.0

Version	CPU (Fr)	Flash	RAM	Wireless	Switch	boot_wait	JTAG	USB
1.0	Broadcom4710 125MHz	4 MB	16MB	Broadcom (mini-PCI)	ADM6996l	OFF	NO	NO
1.1	Broadcom4710 125MHz	4 MB	16MB	Broadcom (integrada)	ADM6996L	OFF	YES	NO
2.0	Broadcom4712 200MHz	4 MB	16MB	Broadcom (integrada)	ADM6996L	OFF	YES	NO
2.2	Broadcom4710 200MHz	4 MB	16MB	Broadcom (integrada)	BCM5325	OFF	YES	NO
3.0	Broadcom4710 200MHz	4 MB	16MB	Broadcom (integrada)	BCM5325	OFF	YES	NO
3.1	Broadcom4710 216MHz	4 MB	16MB	Broadcom (integrada)	BCM5325	OFF	YES	NO
4.0	Broadcom5352 200MHz	4 MB	16MB	Broadcom (integrada)	IN CPU	OFF	YES	NO
5.0	Broadcom5352 200MHz	2MB	8MB	Broadcom (integrada)	IN-CPU	OFF	YES	NO
6.0	Broadcom5352 200MHz	2MB	8MB	Broadcom (integrada)	IN-CPU	OFF	YES	NO
8.0	Broadcom5352 125MHz	2MB	8MB	Broadcom (integrada)	IN-CPU	OFF	YES	NO

Tabla 3.1: Características internas del Router Linksys

Para elegir el mejor router a utilizar, se puso especial cuidado en lo referente a la memoria RAM y Flash, puesto que son las dos memorias en que se trabajaran, y también en los datos de CPU. Es por esto, dentro de las posibilidades, es que se utilizo el router linkys modelo wrt54G v2.0 ya que fue el router de mejor capacidad que se encontraba en el mercado al momento de comprar los materiales.

Aparte de las características técnicas de memoria que se tuvieron que tomar en cuenta, también un punto muy importante fue el echo que se necesitaba un router que soportara el sistema operativo (frimware) OpenWrt, el cual es sumamente importante para el desarrollo de la tesis, ya que en este frimware se basa en su totalidad la tesis y el estudio de factibilidad de los router.

Otra razón por la cual se escogió este equipo, es por que había una gran cantidad de materia sobre él, para el cambio del frimware y sobre el soporte para los problemas que se podían presentar para el cambio del frimware.

La constitución interna del router se puede apreciar en la figura 3.2, la cual es una foto tomada a la placa del routes, en ella se pueden apreciar sus componentes as importantes como lo son la memoria flash cpu, ram, etc.

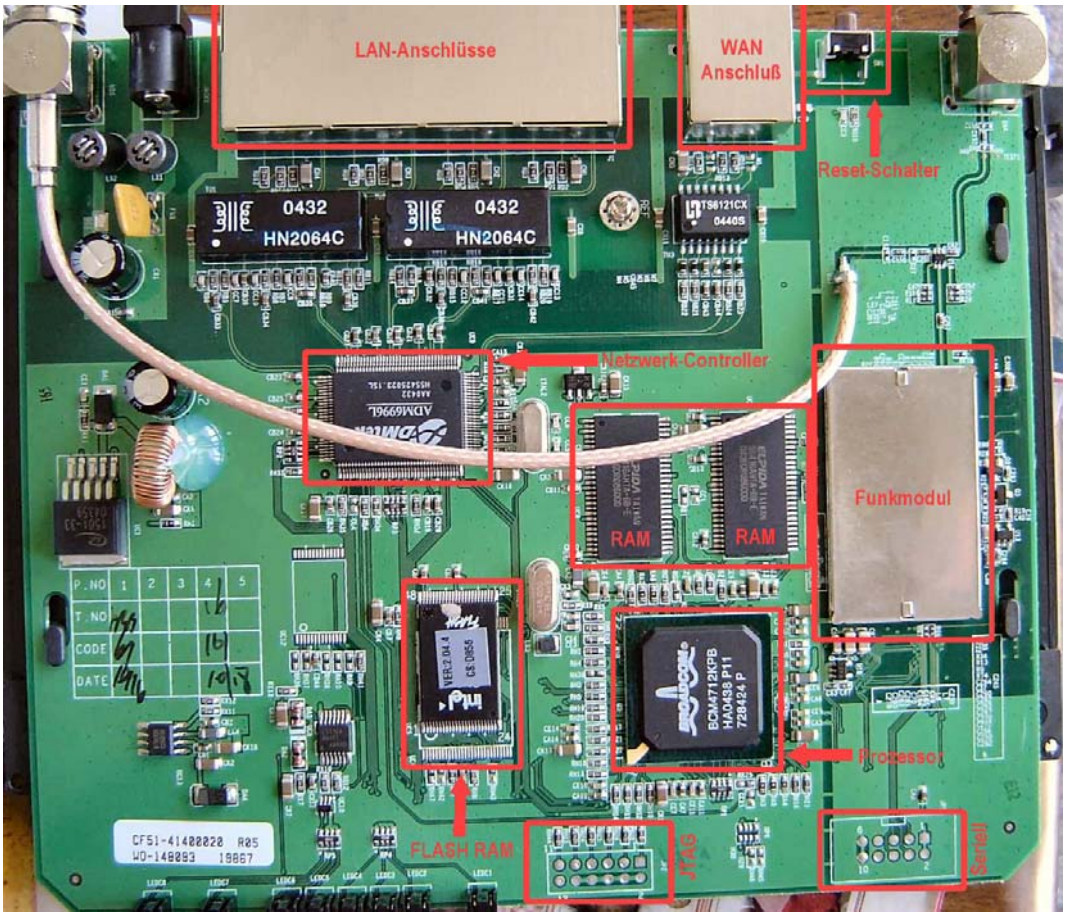


Figura 3.2: Placa impresa del router linksys.

En la figura 3.2 podemos apreciar claramente que posee dos chips de memoria, aparentemente cada una de 8MB, para así lograr los 16MB de ram que tiene el router para trabajar sobre él. La tartera wifi, que permite la radicación de la señal de Internet, se puede apreciar en el modulo que dice Funkmodul. También se apreciar fácilmente los conectores JTAG, que corresponden a los puertos de consola que tiene el router para ingresar por cualquier desperfecto que tengo, o si fuese necesario gestionar el equipo directamente de la bios.

A continuación se realizara una descripción un poco mas detalladas de las partes más importantes de la placa impresa:

Conectores LAN: Zócalos de conexión para red cableada, con cable ethernet y conectores RJ-45. Este modelo cuenta con 4 conectores para red lan, para conectar los usuarios cableados de mi red.

Conector WAN: Zócalo de conexión a Internet, con conector RJ-45. Es donde llegara el cable de red que nos proveerá de la Internet para nuestro router.

Resert: Botón que con el frimware original servia para dejar de fabrica el router, por si tenia algún problema. Con el nuevo frimware, este botón se utilizaba para dejar el router en su modo failsafe, que nos permite entrar vía telnet al router cuando la sesión SSH se haya perdido por algún motivo.

Flash RAM, RAM: Estas son las memorias en donde se trabajara para obtener los resultados y realizar las pruebas que se requieran, en la memoria flash es donde se cargar el frimware requerido (OPENWRT), y sobre la memoria RAM se trabajara con los programas de ejecución como lo es el openser. Las capacidades de estas memorias son sumamente importantes, ya que si las capacidades no son las adecuadas algunos de los programas que se requiere utilizar no se podrán utilizar de forma adecuada y correcta, ya que los espacios necesarios para que corran no serán las adecuadas.

3.2.1.1 Tabla de características técnicas.

A continuación en la tabla 3.2, se presentan las características técnicas del fabricante de este modelo de router inalámbrico (Linksys WRT54G V2.0):

General	
Tipo de dispositivo	Enrutador inalámbrico
Factor de forma	Externo
Anchura	18.6 cm
Profundidad	20 cm
Altura	4.8 cm
Peso	0.5 kg
Conexión de redes	
Tecnología de conectividad	Inalámbrico, cableado
Conmutador integrado	Conmutador de 4 puertos
Velocidad de transferencia de datos	54 Mbps
Banda de frecuencia	2.4 GHz
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g
Protocolo de conmutación	Ethernet
Protocolo de gestión remota	HTTP
Modo comunicación	Dúplex pleno
Indicadores de estado	Actividad de enlace, alimentación
Características	Capacidad duplex, protección firewall, puerto DMZ, soporte de DHCP, soporte de NAT, asistencia técnica VPN, Stateful Packet Inspection (SPI), filtrado de paquetes, filtrado de dirección MAC, cifrado de 256 bits
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g, Wi-Fi CERTIFIED
Antena	
Cantidad de antenas	2
Expansión / Conectividad	

Interfaces	1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 4 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x red - Radio-Ethernet
Diverso	
Cables (Detalles)	1 x cable de red
Algoritmo de cifrado	Ncriptación de 64 bits WEP, WPA2
Cumplimiento de normas	CE, IC, FCC
Alimentación	
Dispositivo de alimentación	Adaptador de corriente - externo
Software / Requisitos del sistema	
Software incluido	Norton Internet Security
Sistema operativo requerido	Microsoft Windows 98SE/2000/ME/XP
Tipo mínimo de procesador	Intel Pentium 200 MHz
Capacidad mínima RAM	64 MB
Dispositivos periféricas / interfaz	CD-ROM
Detalles de los requisitos del sistema	Pentium - 200 MHz - RAM 64 MB
Parámetros de entorno	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	10 - 85%

Tabla 3.2: Características técnicas linksys WRT54G V2.0

3.2.1.2 Consideraciones importantes

Si observamos la tabla 3.1 podemos apreciar las capacidades, en cuanto a memoria ram y flash de los distintos router que soportaban el frimware requerido, con respecto ha esta lista es que se eligió el modelo mas apropiado para los requerimientos deseados, el escogido es el WRT54G V2.0, por las capacidades de memoria que poseía (Flash 4MB; Ram 16MB), ya que el

openwrt ocupa una memoria de 4786K y con una memoria de 16MB en Ram era suficiente para instalar la versión whiterussian RC6, la cual estaba disponible en la pagina web http://downloads.openwrt.org/whiterussian/. También se utilizaron otras versiones, pero con bastantes inconvenientes, por ejemplo, se utilizo la versión Kamikaze la cual no tenia soporte para wireleess y además ocupaba demasiada memoria Ram, lo cual no permitía correr correctamente el openser, programa que se describe en el capitulo 2, y sin éste programa no se podía continuar el desarrollo de la tesis, así que por lo tanto para este router se utilizo la versión whiterussian RC6, la cual utilizaba menos memoria Ram y permitía correr sin ningún problema el openser dentro del router así como una serie de programas necesarios para el desarrollo de la tesis.

Además, este router fue escogido por su fácil obtención en el mercado, ya que al momento de la compra era uno de los router que estaba a disposición para ser utilizados. Cabe mencionar que no todos los router de la lista antes mostrada estaban a disposición en el mercado chileno-valdiviano para la compra, lo que facilito también la decisión de la compra de este producto.

Cabe mencionar, que otro de los parámetros que se tomo en cuenta para la obtención de este router para su anales en el proyecto de esta tesis, es que se podría encontrar documentación que respalde este estudio, aunque no era información oficial y algunas son simplemente especulaciones sobre los métodos, se podría encontrar con bastante facilidad en los foros información sobre los cambios de frimware de este router como también los problemas mas recurrentes con los que podría haberme encontrado al momento de trabajar con él. También mencionare que el desarrollo de la tesis en si, no se encontraba documentación ni tampoco se sabia que la propuesta del esquema podría resultar, solo se contaba con estudios hechos con asterisk, pero para la tesis se utilizo el openser.

Este router resulto ser muy estable y robusto ideal para la arquitectura que se propuso, el único gran inconveniente era su limitada memoria, que al instalarle una versión mas completa de openwrt, no permitía correr el openser, es por esto que se busco en una segunda fase un router con mucha mas capacidad, tanto de memoria flash como Ram, es así como se llega al router NETGEAR WGT634U, el cual se detalla a continuación.

2.7.2 Router Netgear

La figura 3.3 nos muestra la estructura física del router nertgear WGT634U, que fue el segundo router utilizado para el desarrollo de esta tesis. Las características que determinaron la utilización de este router, las podemos apreciar fácilmente en la tabla 3.3, que nos muestra las capacidades de memoria y procesador que cuenta este router. Cabe destacar que una de los motivos por que se escogió este router, es que tenia soporte para el frimware OPENWRT el cual es el utilizado para el desarrollo de esta tesis.

Figura 3.3: Router Netgear WGT634U

Cabe mencionar que la tabla 3.3 solo muestra los modelos de router netgear que soportan el frimware openwrt.

Modelo	CPU (Fr)	Flash	RAM	Wireless	Switch	Serial	JTAG	USB
DG834G	Texas Instruments AR7 150MHZ	4MB	16MB	ACX111 (VLYNQ)	Marvell 88E6060	Yes	No	No
WG302	Intel IXP422 266MHz	8MB	16MB	1x Atheros (mini-PCI)	None	Yes	?	No
WG602	Broadcom 4712 200MHz	2MB	8MB	Broadcom (integrated)	None	Yes	Yes	No
WGR614	Atheros 2312 180MHz	4MB	16MB	integrated Atheros	?	?	?	No

WGT624	Atheros 2312 180MHz	4MB	16MB	integrated Atheros	Marvell	Yes	Yes	No
WGT634U	Broadcom 5365 200MHz	8MB	32MB	Atheros (mini-PCI)	in CPU	2x 3.3v	No	1x v2.0

Tabla 3.3: Características Internas Router Netgear WGT634U

Para escoger el router que se utilizó, se puso especial cuidado en los parámetros de memoria RAM y flash, que sean superiores a las del linksys, para realizar pruebas y se puedan correr sin ningún problema una cantidad mayor de programas. Si ponemos atención a la tabla nos damos cuenta que el modelo WGT634U cuenta con casi el doble de la memoria del router linksys, lo que nos permite contar con mas espacio para correr distintos programas y por su puesto una versión mucho mas potente del Openwrt. La versión utilizada en este router es la Kamikaze, cuya especificaciones se darán a conocer en el capitulo 4 con mas detalle.

Una vez más, también se tomo en cuenta la cantidad de materia que existiera sobre la instalación y solución de problemas que tuviera a disposición sobre este router. Sin contar con una característica muy importante con la que cuenta este router, la que no poseía el router linksys que se utilizo en primera instancia. El router wgt634u cuenta con una conexión seria a trabes de un cable que se puede fabricar fácilmente y que posee un conector J7. Este cable es de vital importancia para el cargado del frimware que se requiere instalar, ya que éste nos permite entrar por consola al router, manejándonos directamente en la bios del router, y con modo de comandos, con una conexión a través del puerto seria, se entro al router (La explicación de cómo se cambio el frimware a la maquina, se da a conocer con detalles en el capitulo 4).

Este cable lo podemos ver en la figura 3.4, cabe mencionar que el cable esta creado a través de un cable de celular, el DKU5, al cual se le cambio el conector y a través de un tester y con ensayos de prueba y error se encontró la combinación correcta a los cable que se debían conectar en GND, TX y RX, dejando siempre libre el conector de Vcc. Este cable trabaja con un voltaje aproximado 3.3 (v) que deben ir a las patas de Tx y Rx, dependiendo de la acción que se este ejecutando. Mencionamos igual que este cable es de vital importancia al momento de

cambiar un frimware, ya que cualquier problema que se llegase a presentar, es muy fácil arreglar el router a través de esta conexión de consola.

Figura 3.4: Cable de conexión serial

3.2.2.1 Estructura Interna del Router

La figura 3.5 nos muestra la placa impresa del router netgear wgt634u, en la cual se pueden observar claramente cada parte del router, las cuales algunas, se detallaran a continuación.

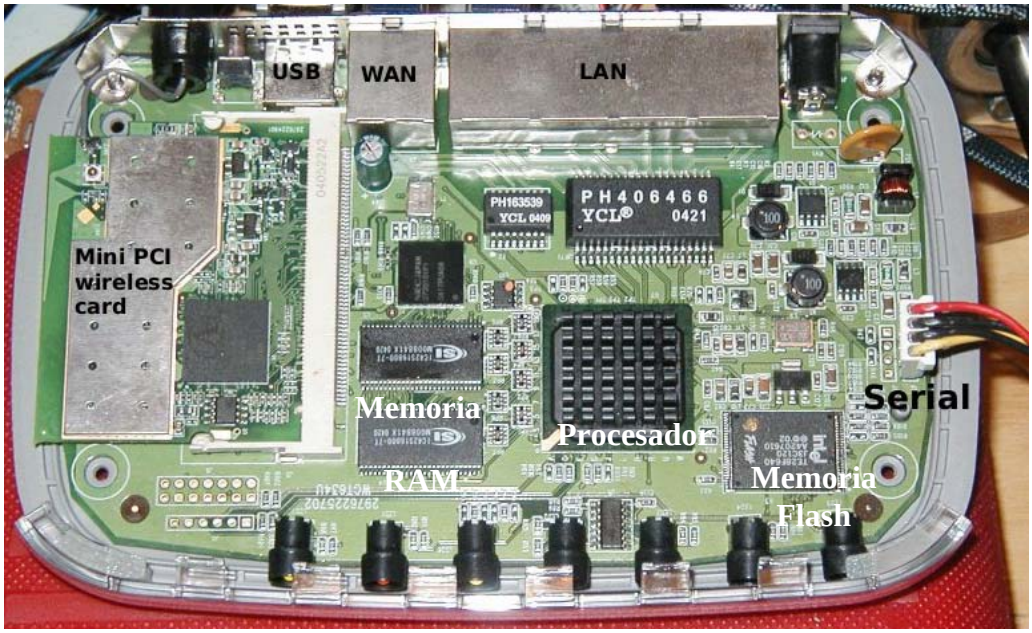


Figura 3.5: Router Netgear WGT634U

Mini PCI Gíreles Card: Corresponde a la tarjeta inalámbrica wifi. Cabe mencionar que esta tarjeta se puede cambiar con facilidad y la que trae integrada es para 108 Mbps, una velocidad excelente para las transmisiones de voz.

Memoria Ram: Dos stot de memoria, cada una de 16MB, la cual se utilizara para el funcionamiento de los programas que se desean utilizar.

Memoria Flash: 8MB de memoria la cual nos permite cargar el frimware necesario para el desarrollo del trabajo de titilación.

Procesador: Unidad central y principal del router, encargada de procesar los datos requeridos para su correcto funcionamiento.

Puerto Serial: Característica especial de este router, la cual nos permite visualizar lo que esta pasando directamente en la BIOS del router, y nos permite solucionar cualquier problema que se nos presente además de realizar los cambios que sean necesarios para la utilización del router, como es el caso del cambio de frimware. Para utilizar este puerto seria es necesario confeccionar un cable seria, el cual se puede ver en la figura 3.4.

Puertos LAN y WAN: El puerto WAN es el que nos sirve para conectarnos a Internet y además es por donde se puede enviar el frimware a trabes de TFTP (ver capitulo 4). LAN es e puerto en donde se conectan los usuarios cableados de la red al router.

USB: Otra característica especial y de mucha utilidad para el desarrollo de la tesis. Este router tiene la facilidad de coactarle algún dispositivo externo de almacenamiento, lo que nos permite una ampliación de sus capacidades y además la facilidad de cargar un servido FTP sobre él, característica que no posee el router linksys.

Como se puede apreciar comparativamente, el router NETGEAR tiene muchas mas funcionalidades y una mejora de sus capacidades con respecto al LINKSYS es por ellos que se decidió trabajar sobre él para el desarrollo de este trabajo de titulación.

3.2.2.2 Tabla de características Técnicas

A continuación, la tabla 3.4 nos muestra las características técnicas y de funcionamiento del fabricante de nuestro Router NEGEAR WGT634U.

General	
Tipo de dispositivo	Enrutador inalámbrico
MPN	WGT634UFS
Factor de forma	Externo
Dispositivos integrados	Antena
Anchura	17.5 cm
Profundidad	11.9 cm
Altura	2.8 cm
Peso	0.3 kg
Conexión de redes	
Tecnología de conectividad	Inalámbrico, cableado
Conmutador integrado	Conmutador de 4 puertos
Velocidad de transferencia de datos	108 Mbps
Banda de frecuencia	2.4 GHz
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g, 802.11 Super G
Protocolo de direccionamiento	Direccionamiento IP estático
Formato código de línea	DBPSK, DQPSK, CCK, 64 QAM, BPSK, QPSK, 16 QAM, OFDM
Método de espectro expandido	OFDM
Red / Protocolo de transporte	TCP/IP, PPTP, L2TP, IPSec, PPPoE
Indicadores de estado	Estado puerto, actividad de enlace, velocidad de transmisión del puerto, alimentación, modo de prueba
Características	Protección firewall, encaminamiento, auto-sensor por dispositivo, soporte

	de DHCP, soporte de NAT, Stateful Packet Inspection (SPI), prevención contra ataque de DoS (denegación de servicio), filtrado de contenido, servidor DNS dinámico, activable, pasarela VPN
Cumplimiento de normas	IEEE 802.11b, IEEE 802.11g
Antena	
Cantidad de antenas	1
Expansión / Conectividad	
Interfaces	1 x Hi-Speed USB - 4 PIN USB tipo A 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN) 4 x nodo de red - Ethernet 10Base-T/100Base-TX - RJ-45 1 x red - Radio-Ethernet
Diverso	
Cables (Detalles)	1 x cable de red
Algoritmo de cifrado	WEP de 128 bits, ncriptación de 64 bits WEP, WEP de 40 bits, WPA
Método de autentificación	Identificación de conjunto de servicios de radio (SSID)
Cumplimiento de normas	UPnP
Alimentación	
Dispositivo de alimentación	Adaptador de corriente - externo
Software / Requisitos del sistema	
Software incluido	Controladores y utilidades
Sistema operativo requerido	Microsoft Windows NT, Microsoft Windows 98SE/2000/ME/XP
Parámetros de entorno	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	10 - 85%

Tabla 3.4: Características técnicas de fabricante Router WGT634U

3.2.2.3 Consideraciones Importantes

Es importante mencionar que la decisión de utilización de este router es por tener mas espacio en sus memorias y por su facilidad de tener un dispositivo de almacenamiento externo para poder utilizarlo en caso de que se requiera mas espacio o para cualquier utilización posterior a la tesis. También se debe mencionar que como este router cuenta con mas espacio de memoria que el router linksys, se le instala la versión Kamikaze del openwrt, ya que en el anterior nos utilizaba todo el espacio de memoria ram, en este queda suficiente espacio para correr los demás programas y sobra bastante memoria, lo cual es una ventaja a la hora de hacer correr el openser ya que anda con mas eficiencia y tiene un rendimiento mucho mas alto.

Además de estas características, la facilidad de poder entrar a la consola a través del puerto serial del router lo hace un router mucho mas seguro y estable que el linksys ya que ante cualquier problema que se presente en el funcionamiento del router, es fácil tratar de identificarlo y poder repararlo gracias a esta facilidad, y sin contar que también cuenta con el sistema del modo failsafe que nos permite entrar vía telnet al roter por cualquier problema que se presente en el funcionamiento normal del router.

Una desventaja, pero esto es mas de la versión del frimware soportado, es que no trae activado el modo Bootwait, que nos permite cambiar el frimware vía TFT sin ningún problema, pero la utilización del puerto seria soluciona fácilmente este pequeño inconveniente que tiene nuestro router NETGEAR WGT634U.

También es importante mencionar, que el soporte que se tenia para este router en Internet, era bastante pobre comparado con el del linksys, además que muchas de las cosas que se requerían hacer al router todavía estaban en etapa de prueba, de echo la misma pagina del OPEWRT lo afirma, que esta en periodo de prueba. Pero para lo que se necesitaba realizar, era suficiente la información y afortunadamente todo lo que se requería funciono sin ningún problema en el sistema implementado.

3.3 Softphone utilizados

Uno de los puntos más importantes a considerar al momento de escoger algún software para utilizarlo como softphone, es que posea la característica de soportar el protocolo IPv6 y que sea capas de trabajar con las dos versiones de protocolo IP. Es por esto que se utilizó para las pruebas de comunicación entre equipos terminales el softphone eyebeam (Versión 1.5.13), que posee soporte IPv6 y es de fácil utilización y se puede encontrar en el mercado fácilmente a un precio bastante módico.

Es importante destacar que este softphone tiene soporte para Windows XP y no para Linux, ya que la plataforma universal de utilización de los clientes comunes de Internet y de un PC es Windows, ahora para Windows Vista aun no se ha actualizado el softphone, pero lo importante para el desarrollo de la tesis es que el software tengan soporte para IPv4 e IPv6 y la versión eyebeam 1.5.13 tiene soporte para IPv4 e IPv6.

También destacare que este software fue obtenido gracias a un grupo de trabajo de asterisk, que desarrolla esta PBX para la versión IPv6.

Eyebeam es un software que nos permite realizar llamada y video conferencia sobre el protocolo IP. Es esto lo que se llama VoIP y VideoIP, que corresponde a la nueva forma de comunicación que se esta dando, gracias a la masificación de Internet en todo el mundo. En particular, el eyebeam trabaja directamente con paquetes de trafico SIP y que tiene, ya la versión 1.5.13, soporte para el nuevo protocolo IPv6 que a medida que pasa el tiempo nos damos cuenta que se esta haciendo una gran necesidad que se masifique este protocolo de comunicación.

A continuación de describirá paso a paso los métodos que se utilizaron para configurar este software y la forma en que se utilizo para realizar las pruebas necesarias para lograr los objetivos que se esperaban para esta tesis.

No debemos perder de vista que un softphone no es nada mas que un programa que simula a un teléfono tradicional, dentro de un computador, así que para ello necesitamos como requisito mínimo un parlante para escuchar la llamada y un micrófono que es por donde podremos comunicarnos con la otra persona con la que se requiere comunicar.

3.3.1 Configuración Softphone

Para configurar el softphone, lo primero que se debe hacer es instalarlo, asiendo clic en el instalado, como lo muestra la figura 3.6.

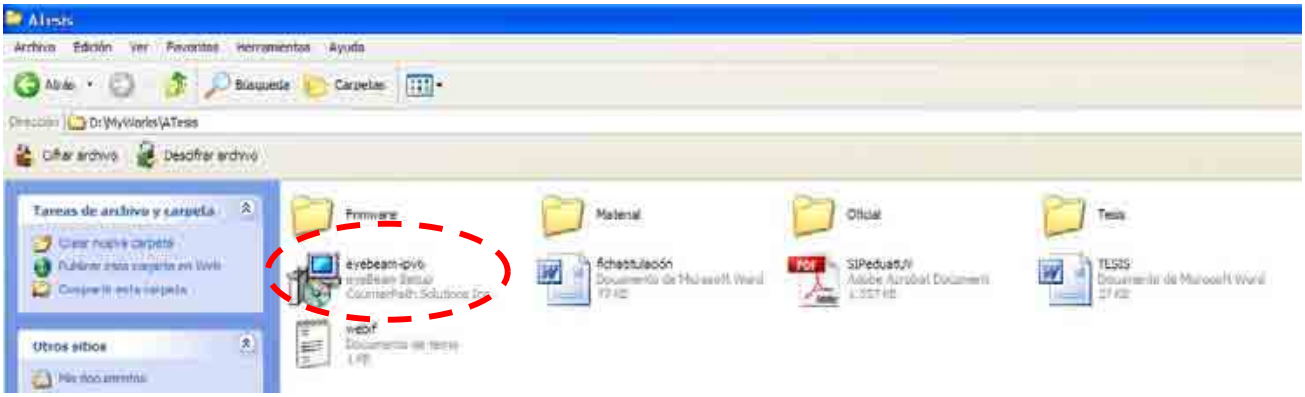


Figura 3.6: Instalador eyebeam-ipv6

Luego de esto aparece la pantalla donde comienza la instalación, donde como es tradicional en los programas, hay que presionar siguiente hasta que termine la instalación, como lo muestra la figura 3.7.

Figura 3.7: Ventana del Instalador

Como observamos, la instalación de este software es igual que la de cualquier programa común, ahora una ves terminada la instalación, nos debería aparecer el siguiente programa corriendo en nuestro computador. Ver figura 3.8

Figura 3.8: Softphone Eyebeam 1.5.13

Sobre este programa, buscamos la opción de *"SIP Account Setting"* como se ve en la figura 3.9

Figura 3.9: Primer paso de la configuración.

Luego de hacer clic en esta opción nos aparecerá la ventana que muestra la figura 3.10, a la cual hay que seleccionar un canal y configurarlo presionando la opción “Add”. Luego de haber echo la configuración nos aparecerá el dominio y el username que se esta utilizando para el trafico de las llamadas, podemos observar que se pueden tener mas de un dominio, pero para el desarrollo de la tesis solo se utilizara uno.

Figura 3.10: Segundo paso de la configuración

Continuando con la configuración del softphone, cuando se llega a este punto, se le configura la ip del servidor SIP. Para nuestro caso es la IP del router la que se le configurara, con el cuidado que si estamos en IpV4 se le colocara un IpV4 y si trabajamos con IpV6 se le colocara una IPv6, ya que el router tiene ya configurado las dos versiones de IP existentes y tiene, por tanto soporte para estas dos versiones de protocolos.

En el casillero de *Display Name*, va un nombre cualquiera que reconozca al usuario. Este nombre es el que registra el openser para llevar un registro de los usuarios que usan el sistema.

En la casilla *User Name*, se coloca el nombre de usuario que es el asignado por la central, en este caso openser, que por lo general es un número de teléfono, pero como estas son solo pruebas de laboratorio se le coloco “test 1”. Es importante destacar que para las pruebas realizadas y el esquema montado en el laboratorio no fue necesario contar con un nombre de usuario y contraseña, por lo que se utilizo en su modo por defecto, que permite a cualquier usuario conectado dentro de la misma LAN coactarse a la central y traficar llamadas telefónicas sin problema. Ahora si se desea algo mas elaborado con una cierta cantidad de usuarios conectados y llevar un control de estos, debemos cargarle una base de datos MSQL, en la cual se guardan los usuarios, esta base de datos esta disponible por el mismo programa openser, para configúrala e instalarla, pero para el desarrollo de este trabajo de tesis no fue necesario instalarla.

En la casilla *“Password”*, se coloca la password que se coloco en la base de datos. Para este caso en particular no se coloca cualquier cosa por que se esta utilizando el medio por defecto del openser que permite la comunicación con cualquier password ingresada en el softarwe.

En la casilla *“Domain”*, Aquí va la dirección IP donde se encuentra alojado el openser. Para nuestro caso, es la dirección del router. Vale la pena observar que si uno le coloca la dirección del router con respecto a la LAN como con respecto a la WAN funciona igual, ahora es importante decidir cual va ha ser el tipo de comunicación que se realizara, para esta tesis solo era importante comunicar dos computadores dentro de la misma LAN así que por esto se el coloco la IP de la LAN, ahora importante también destacar que si utilizamos IPv6 es aquí donde debemos colocar la IP, para que funcione en IPv6.

Con lo respecto al *“Domain Proxy”*, si se esta trabajando en IPv4 se puede colocar el Proxy el mismo dominio o se le puede indicar alguna dirección de dominio Proxy. Ahora si se trabaja con IPv6 se debe especificar la dirección ipv6, que para este caso es la misma que la del router.

Todo esto se puede ver en la pantalla que muestra la figura 3.11, en la cual aparece la configuración por defecto que tiene uno de los usuarios utilizados en la pruebas de laboratorio que se le desarrollaron al sistema implementado.

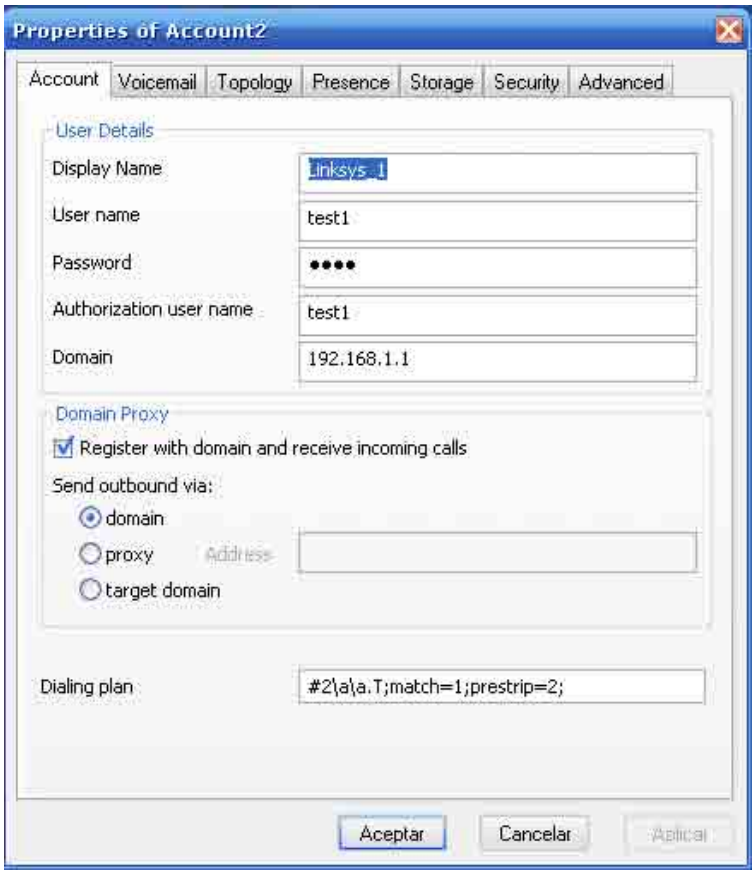


Figura 3.11: Propiedades de configuraron del eyebeam

Es importante destacar que la utilización del softphone, como la configuración de los router, se realizo pensando solo en saber si era posible montar este esquema en un router, analizando las potencialidades del router y comunicando a los equipos dentro de la misma LAN, es por esto que las configuraciones se hicieron casi por defecto y de forma mínima, resguardando solo los objetivos principales del trabajo de titulación.

En los demás capítulos se detallan las configuraciones del openwrt, la instalación y utilización de este software en los router.

CAPITULO IV

FRIMWARE OPENWRT Y METODOLOGIA DE INSTALACIÓN

4.1 Antecedentes

En el presente capitulo, se presenta la metodología utilizada para la instalación de los sistemas operativos (frimware) en los routers, que se utilizaron como la metodología de configuración y un detalle de todos los pasos o por menores que ocurrieron en la instalación en cada router.

Es importante mencionar que el frimware utilizado, el OPENWRT es un frimware basado en Linux, de libre distribución y además de código abierto, lo que nos permite realizar cambios y avances en el kernel del sistema operativo, siendo esta una gran ventaja para el desarrollo de aplicaciones y modificaciones para el desarrollo del trabajo de titilación, pero lo mas importante de destacar, es que poseía módulos de fácil instalación, que con un simple comando se podían instalar y así poder modificar el kernel del sistema operativo sin ningún problema, como sucedió para la instalación del soporte de IPv6 y también la instalación del Openser, que fueron los programas que se utilizaron para lograr los objetivos.

A continuación se describirá paso a paso y para cada router la metodología de instalación, y el detalle de su configuraron:

4.2 Router Linksys WRT54G

En el caso de la instalación del frimware para este router, ya se contaba con un frimware openwrt versión whiterussian RC6, pero este frimware fallo y tubo que ser vuelto a instalar, con lo que se intento probando con la versión Kamikaze, la cual esta instalada en el router netgear, pero el problema fue que la versión caminase no cuenta con entorno grafico, lo que se conoce como webif, lo cual había que cargarle una versión que se encontraba disponible en la pagina web de Openwrt, la versión X-wrt, con lo que la memoria de trabajo del router se encontraba casi

en los limites, con la dificultad de que al momento de arrancar el programa Openser (ver capitulo II), el router no contaba con la memoria necesaria para que funcionara de forma normal. Con lo que se tubo que volver a instalar la versión whiterussian RC6 al router, la cual se detalla en los siguientes pasos.

Es importante mencionar, que tanto en el frimware original como en el whiterussian RC6 de openwrt, se pueden realizar las actualizaciones a trabes del soporte Web que traen los frimware, ahora, se opto en el trabajo de tesis realizar el cambio de los frimware a través de TFTP, ya que se contaba con las imágenes completas para cargar el frimware, lo único que se debía preocupara era tener activado el bootwait, ya que esta opción nos permite cargarle el frimware vía TFTP a lo router si por algún motivo no quedara bien instalado el frimware.

Una vez activado el bootwait se procede a seguir los siguientes pasos:

1. Conectar la puerta Lan del PC que se utilizara, con la puerta WAN del router linksys, ya que ésta puerta es la que envía y recibe información en el linksys, como lo muestra la figura 4.1

Figura 4.1: Conexión del Router

2. Es importante saber cual es la IP del router, es por esto que antes se realiza un PING a la dirección a la cual se va a enviar la información, para este caso el frimware y la dirección a la cual se le envió el PING fue la 192.168.1.1; entonces se debe realizar el comando

"ping 192.168.1.1 –t" en la pantalla cmd (DOS) del sistema operativo windows. El *"-t"* es importante por que así queda enviando pines hasta que uno desee que se detengan. En la figura 4.2 hay un ejemplo.

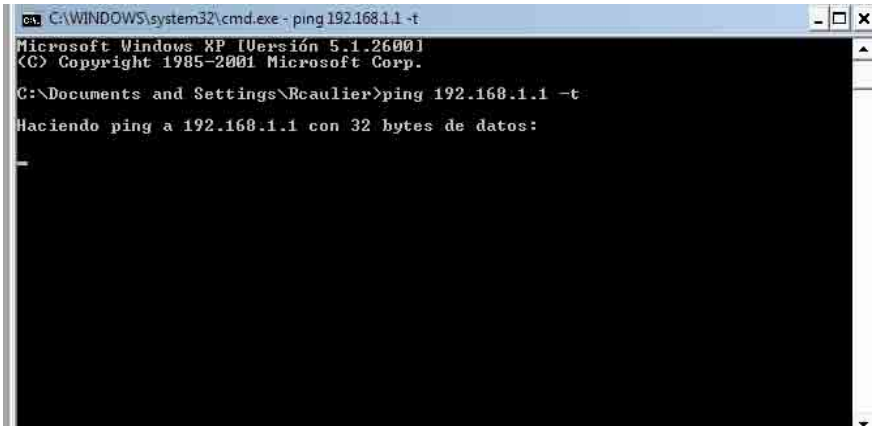


Figura 4.2: ejemplo de paquete ping a la dirección 192.168.1.1

3. Luego de esto, ya sabemos cual es la dirección del router, entonces procedemos ha abrir otra ventana CMD para colocar el siguiente comando *"**tftp** -i 192.168.1.1 PUT (aquí se indica la dirección en donde esta el archivo .bin del frimware)"*, ojo que una ves puesto este comando no se debe NUNCA PRESIONAR ENTER.

4. Luego, desconectar el cable de poder del router y fijarse si la ventana donde se esta corriendo el PING que el host se encuentra inaccesible. Una vez ocurrido esto se debe volver a encender y esperar hasta que se prenda la primera luz y que en la ventana donde esta corriendo el PING aparezca el primer PING de respuesta y justo en ese instante se debe presionar "ENTER" en la ventana en donde se tiene el comando con el TFTP activado. Una vez cargado el frimware ya esta listo para ser utilizado. En el caso de que no se haya alcanzado a cargar el frimware, se puede seguir intentando todas las beses que sea necesario.

Con este procedimiento se logro cambiar el frimware que tenia el router, al frimware que se requería para el trabajo de titilación. Luego de esto la configuración para esta versión de frimware fue bastante fácil ya que casi todo venia por defecto, haciendo referencia al webif (entorno grafico de web), y mayores configuraciones no se le realizaron. Reconocía sin

problemas la internas inalámbrica y se podía trabaja tanto en modo grafico como en modo comandos.

La figura 4.3 nos muestra el frimware Openwrt versión whiterussian RC6, ya instalada en el router y funcionando sin problemas tanto la interfaz grafica (figura 4.4) como el modo de consola que trae el frimware.

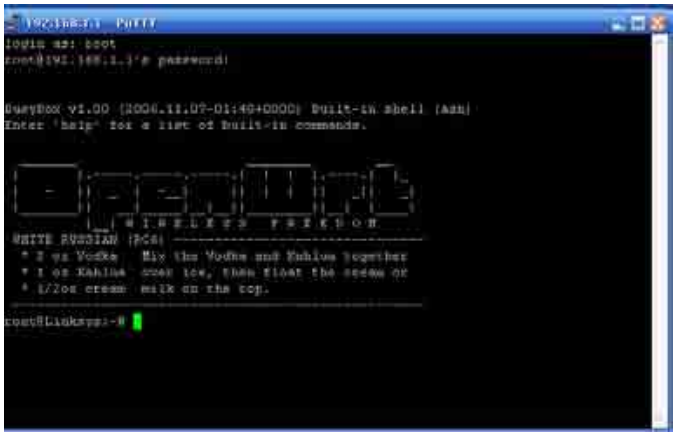


Figura 4.3: Modo consola frimware Openwrt

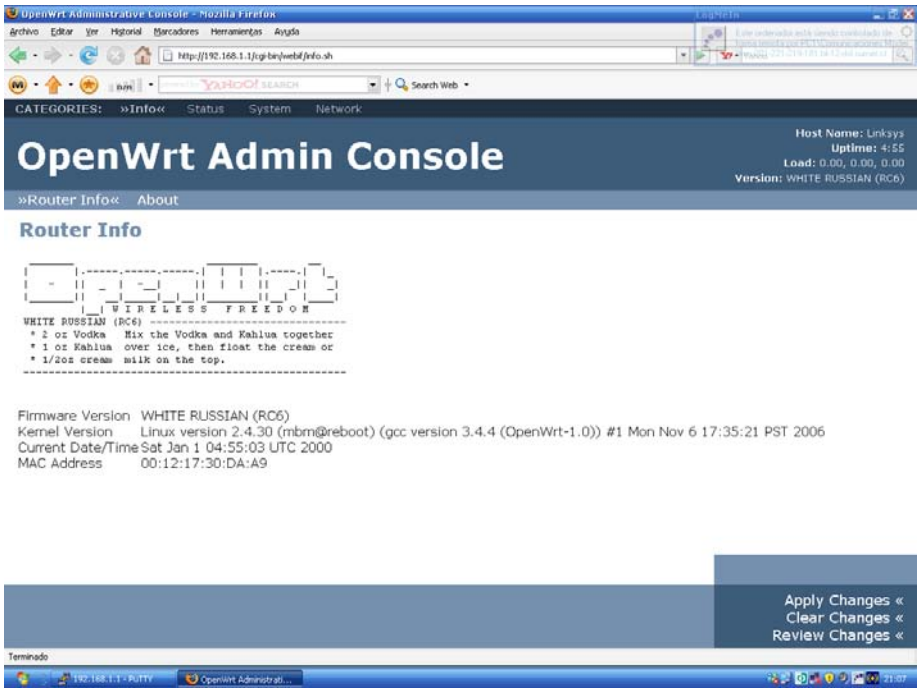


Figura 4.4: Internas grafica frimware Openwrt

En el linksys, en referencia a la instalación y configuración del router, no hubieron mayores complicaciones ya que solamente se necesito cargar el frimware vía TFP y listo, el frimware se encontraba dispuesto a su utilización, en diferencia al router netgear que se tuvo que configurar una ves cargado el frimware Openwrt versión Kamikaze.

4.3 Router Netgear 634U

La instalación del frimware para este router fue un poco mas compleja, ya que el frimware OPENWRT versión Kamikaze no trae habilitada la interfaz Web para el trabajo de configuración, con lo que es necesario instalarla y configurarla todo a trabes de modo comandos, aunque la instalación del frimware en si no es muy complicada pero igual tiene bastantes diferencias con respecto al linksys. El frimware original del netgear es el que se muestra en la figura 4.5

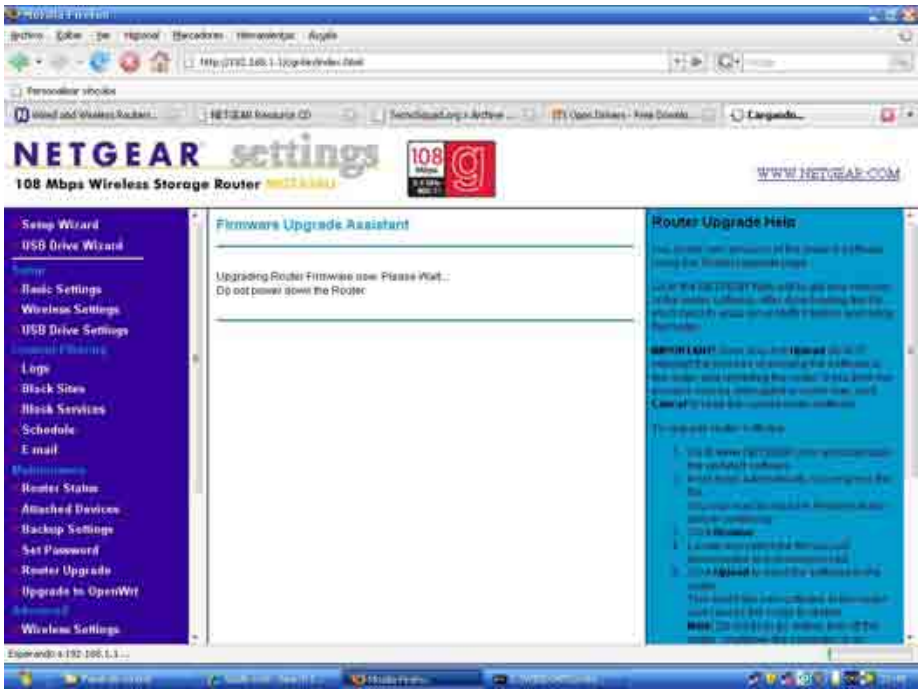


Figura 4.5: Frimware original del netgear

Uno de los motivos de por que se instalo la versión Kamikaze en este router es por que contábamos con mas memoria, se requería probar el sistema implementado con otra versión del mismo frimware y además era la ultima versión disponible para este frimware.

Es importante resaltar que el router Netgear posee un puerto de consola en donde se puede observar lo que esta ocurriendo en la memoria ROM del router, es a través de este puerto que se trabaja para poder configurar las puertas del router y poder solucionar cualquier problema que se presente en el router, además que al intentar instalar el frimware a través del router original, no permite por protección del mismo frimware para evitar el cambio, es por esto que se utiliza igual el puerto de consola. Cuando uno ingresa al puerto de consola a través del Hiperterminal nos encontraremos con lo que muestra la figura 4.6, es en ese instante en donde se presiona la teclas "Ctl-C" con lo que se accede al CFE que corresponde a la ROM del router.

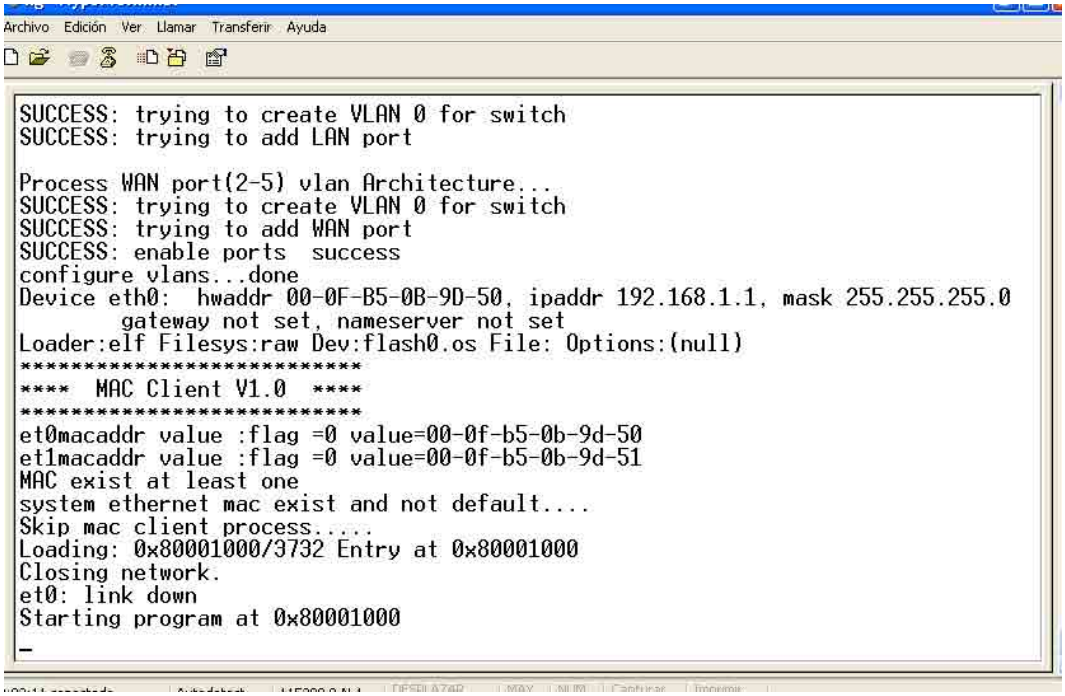


Figura 4.6: Puerto consola del router Netgear

Lo primero que debemos hacer es configurarle a alguna puerta del swicht que tiene el router, una dirección IP conocida para que luego por esta puerta se pueda cargar el frimware gracias a un FTP. La puerta que se escogió en este caso fue la numero 1, es importante destacar que a diferencia del linksys aquí las modificaciones se hicieron por la puertas del swicht del router y no por la puerta WAN. Una ves conectada la puerta y con el cable de consola conectado al router se utiliza el comando siguiente en el modo CFE:

```
CFE> ifconfig eth0 -auto
Device eth0:  hwaddr 00-0F-B5-97-1C-3D, ipaddr 192.168.1.250, mask 255.255.255.0
        gateway 192.168.1.1, nameserver 192.168.1.1, domain foo.com
*** command status = 0
```

Con esto hemos autoconfigurado la puerta eth0 del router y por lo tanto esta activa, ahora manualmente debemos configurarle la ip y mascara que se requiere para la instalación del frimware, la cual es 192.168.1.250 y de mascara 255.255.255.0, de la siguiente forma:

```
ifconfig eth0 -addr=192.168.1.250 -mask=255.255.255.0
```

Una ves echo esto se debe echar a correr un servidor TFTP con el archivo .bin del frimware que se desea cargar al router y en la ventana de comando donde estamos corriendo el CFE se le coloca *"flash -noheader 192.168.1.3:wgt634u/openwrt-wgt634u-2.6-squashfs.bin flash0.os"*, donde la dirección 192.168.1.3 es la dirección del PC donde esta corriendo el servidor TFTP. Una ve de esto se le da *enter* a la instrucción de la ventana CFE y listo, hay que esperar que salga el mensaje que aparece en la figura 4.7.

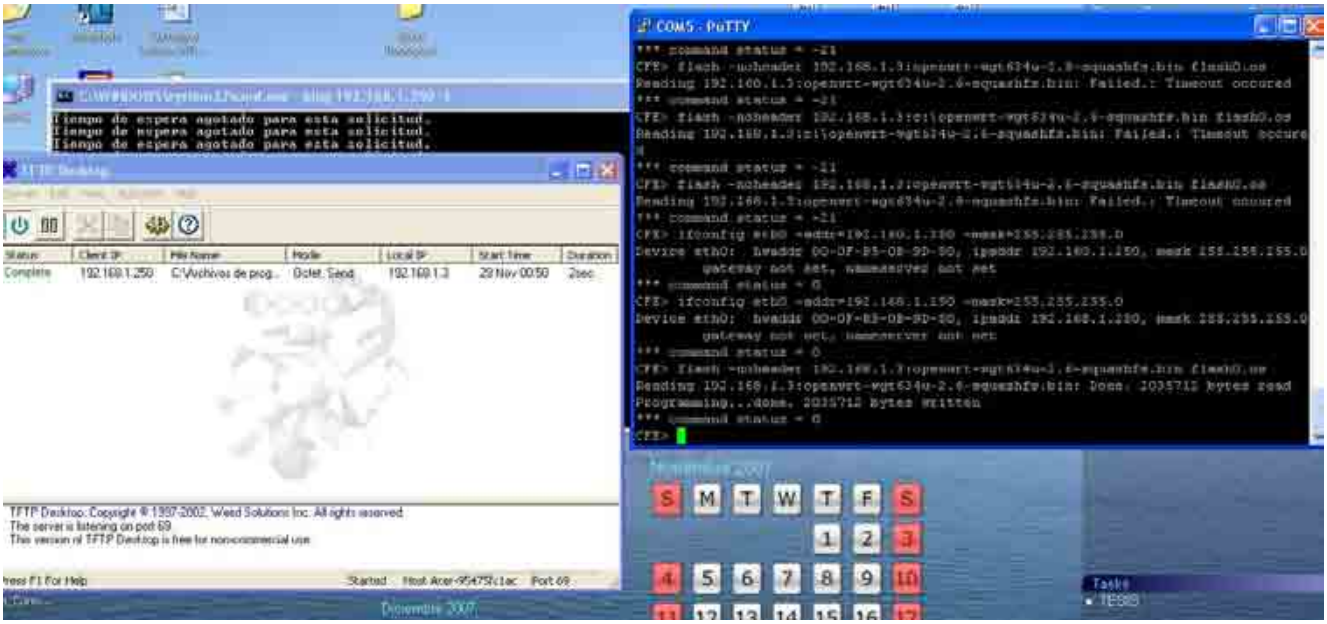


Figura 4.7: Instalación finalizada del frimware en router netgear

En la figura 4.7 podemos observar claramente el servidor TFT corriendo y la ventana del CFE con el comando en ejecución. Una ves realizada esta operación solo basta reiniciar el router, pero por ningún motivo desenchufar de la corriente, si no que hay que aplicarle el comando *"reboot"* para que se reinicie el router de forma normal y hacia pueda arrancar de forma normal.

Es importante tener en cuenta que para ingresar al router a través de SSH debemos asignarle una password al usuario root, es por esto que una ves reiniciado el router lo que se debe hacer es ingresar por telnet a la dirección 192.168.1.1, que corresponde a la dirección del router, y configurarle una password cualquiera al usuario root con el comando "paswrd root xxxx". Con esto ya esta creada la clave y se puede acceder al router a través de SSH. Es importante mencionar que no esta habilitado el servidor DHSP en los router así que es importante que el PC donde se trabaja posea una IP fija para todo el trabajo, que en este caso fue 192.168.1.3.

Todo el trabajo de consola e ingresar a los router a través de SSH o Telnet se realizo con el programa PUTTY que nos permitía trabajar con los router en modo comandos. La figura 4.7b nos muestra ya el frimware instalado y funcionando en el router, pero sin la interfaz gráfica cargada, solo esta operativo el modo comando del Router, el cual es posible verlo con el programa Putty.

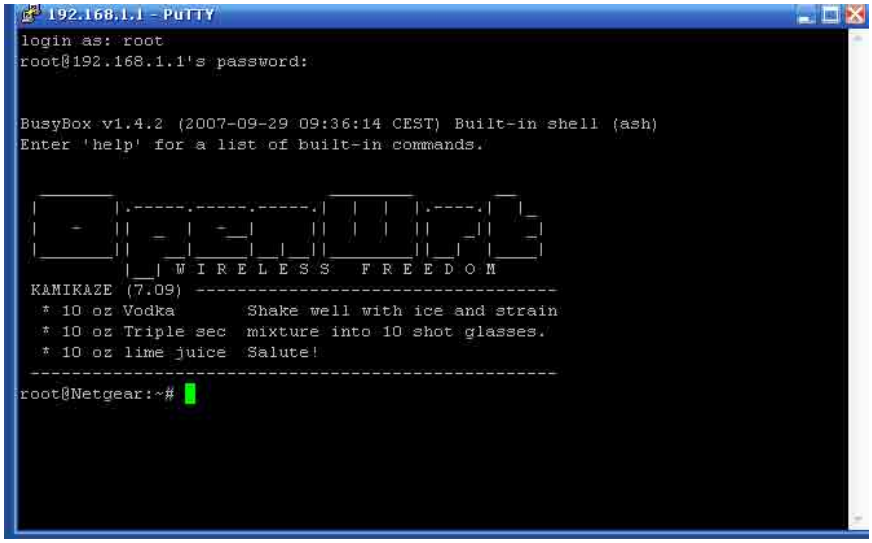


Figura 4.7b: Modo consola frimware Openwrt, versión Kamikaze.

Ahora, para la instalación del webif, que corresponde a la interfaz grafica de la versión Kamikaze, se debe instalar unos paquetes que trae el frimware, ya que no los trae por defecto instalado. Pero antes uno debe, en la ventana de consola, actualizar los paquetes que tiene el frimware con el comando *"ipkg update"* así se actualiza la lista de paquetes y se puede instalar los paquetes del webif. Es importante tener en cuenta que tenemos que estar conectados a Internet para poder actualizar los paquetes e instalar el webif al frimware, es por esto que es recomendable que se trabaje en una red que cuente con el DHSP funcionando así se le asigna una IP por DHSP al router y nos evitamos la configuración, a modo de comandos, de la Internet.

Una vez instalado el frimware, haber actualizado la lista de paquetes y estar navegando, se procedió a instalar el webif, que como anteriormente se señalo corresponde a la interfaz grafica del frimware. Para hacerlo se utilizo el comando *"ipkg install xxxxx -force-overwrite"* en donde se declaraba la dirección Web en donde se encontraba la interfaz Web requerida, que en este caso fue http://downloads.x-wrt.org/xwrt/kamikaze/7.09/brcm47xx-2.6/webif_latest.ipk. La figura 4.8 nos muestra este procedimiento.

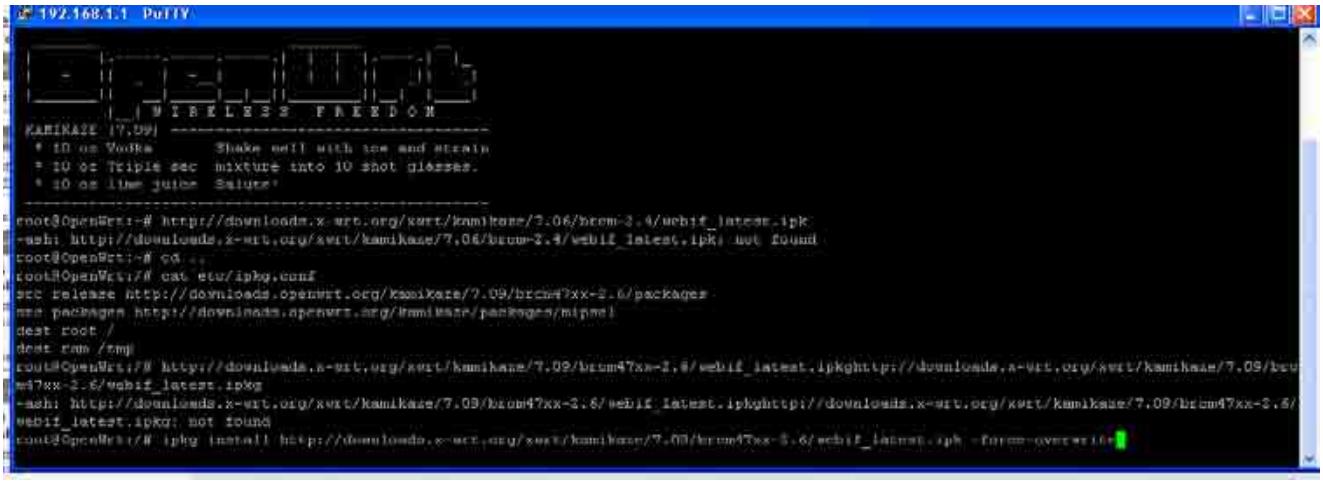


Figura 4.8: instalación webif.

Una vez terminado el proceso que tarda unos breves minutos, el mensaje que muestra lo muestra la figura 4.9.

```
root@OpenWrt:~# ipkg install http://downloads.x-wrt.org/xwrt/kamikaze/7.06/brcm-
2.4/webif_latest.ipk -force-overwrite
Downloading http://downloads.x-wrt.org/xwrt/kamikaze/7.06/brcm-2.4/webif_latest.
ipk
Installing webif (0.3-5) to root...
Installing haserl (0.8.0-2) to root...
Downloading http://downloads.openwrt.org/kamikaze/packages/mipsel/./haserl_0.8.0
-2_mipsel.ipk
Configuring haserl
Configuring webif
Linux OpenWrt 2.6.22 #2 Sun Sep 30 20:38:47 CEST 2007 mips unknown
system type             : Broadcom BCM47xx
cpu model               : Broadcom BCM3302 V0.7
system type             : Broadcom BCM47xx
Linux OpenWrt 2.6.22 #2 Sun Sep 30 20:38:47 CEST 2007 mips unknown
Downloading http://downloads.openwrt.org/kamikaze/7.09/brcm47xx-2.6/packages/Packages
Updated list of available packages in /usr/lib/ipkg/lists/release
Downloading http://downloads.openwrt.org/kamikaze/packages/mipsel/Packages
Updated list of available packages in /usr/lib/ipkg/lists/packages
Downloading http://downloads.x-wrt.org/xwrt/kamikaze/snapshots/brcm47xx-2.6/packages/Packages
Updated list of available packages in /usr/lib/ipkg/lists/X-Wrt
Done.
```

Figura 4.9: Webif instalado.

Es importante observar que el comando que se utilizo tenía la extensión *-force-overwrite,* esto es así puesto que una vez descargado el paquete se debía instalar y el comando para esto es la extensión que se le coloco. Una vez terminado el proceso, la interfaz grafica estará lista para que sea utilizada para configurar el router como se desee. La figura 4.10 muestra el interfaz grafica webif ya en funcionamiento.

Figura 4.10: Entorno grafico del Openwrt versión Kamikaze

Es importante tener en cuenta las diferencias entre las dos versiones de Openwrt, las cuales se verán mas acentuadas en su entorno grafico y se expresan en el apartado 4.4.

4.4 Diferencias entre Versión Kamikaze y whiterussian RC6

Las diferencias que tienen estos dos versiones saltan a la vista al momento de trabajar con ellas y de instalar los programas, pero es importante mencionar que si bien la versión kamikaze es la ultima y esta lista, su entorno grafico se encuentra en desarrollo y hay cosas que todavía no funcionan bien, el X-wrt, que es el nombre de la interfaz grafica posee errores importantes que se resuelven fácilmente utilizando el modo de comandos del router.

Las diferencias son las siguientes:

1. Si comparamos las cantidades de memorias y recursos que utilizan las versiones, la versión whiterussian RC6 ocupaba muchos menos recursos que la versión Kamikaze, es por esto que fue instalada en el router que poseía menos memoria, el linksys, en donde funciono sin ningún problema.

2. La versión Kamikaze no posee un entorno grafico por defecto, hay que instalarlo a diferencia que la versión whiterussian RC6 que tenia su entorno grafico de trabajo predeterminado listo para ser utilizado. Con esto también se puede decir que la versión kamikaze tiene un poco más de dificultad para la configuración, ya que si no se le instala su interfaz grafica no se podrá configurar con facilidad.

3. Desde el punto de vista de la configuración, la versión whiterussian RC6 es mucho mas fácil configurarla, ya que por ejemplo la configuración del wifi esta lista para utilizarla, en cambio en la versión Kamikaze hay que configurarla primero en modo de comandos y luego se puede utilizar.

4. La versión Kamikaze trae habilitadas mas funciones para el monitoreo del trafico y de la cantidad de memoria que esta utilizada en el router, lo que es importante para el trabajo ya que nos entrega información valiosa de forma muy simple, en cambio la versión whiterussian RC6 no trae información del estado del router.

5. La versión Kamikaze trae también más opciones de instalación de programas y paquetes para la mejora de las potencialidades del router, como también un soporte a través del entorno grafico de Asterix por si el usuario quisiera instalarle este programa, cosa que la versión whiterussian RC6 no la trae habilitada.

En resumen, si se necesitara escoger entre las dos versiones del OPENWRT habría que analizar la utilización que se le desea dar al router. Un usuario domestico común debería optar por las versiones whiterussian que están desde las RC1 hasta la RC9, por su fácil instalación y configuración, además de su poca utilización de recursos del router. Ahora si se desea desarrollar alguna aplicación dentro del router, entonces se debe considerar instalar la versión Kamikaze por su gran versatilidad en la utilización de la línea de comando y de su gran apoyo en el entorno grafico, aunque todavía hay algunas opciones que no funcionan en su totalidad. Aunque el inconveniente de esta versión es que necesita un router que posea una memoria RAM y ROM de bastante capacidad.

En el anexo 1 se pueden apreciar fotos de las herramientas de monitoreo del router que están a disposición en la versión Kamikaze del frimware OPENWRT.

CAPITULO V
PRUEBAS Y RESULTADOS

5.1 Antecedentes

En el presente capitulo, se presenta la última etapa del proyecto de tesis, en la que se describen las pruebas realizadas al sistema ya montado y los resultados obtenidos con dichas pruebas. Importante mencionar que las pruebas se realzaron en el laboratorio para ver la capacidades que poseían los router y comprobar si era posible hacer funcionar un sistemas minimizado para la VoiP que consistiera solo de un router, además que sea posible trabajar con los dos protocolos IP existentes hasta el momento, el que se ocupa tradicionalmente IPv4 y el que esta apareciendo actualmente el IPv6.

Las pruebas realizadas solamente fueron las básicas y utilizando los swicht que poseían los router, o sea solo se probó el sistema en una red alámbrica ya que para la red inalámbrica se requiere configurar los frimwares para que funcionen de esta forma. Aunque teóricamente se podría utilizar el sistema de la misma forma para la red alámbrica como para la inalámbrica, ya que el router es el mismo y lo importante es tener bien configurado el router utilizado para que el sistema funcione a la perfección.

Es importante mencionar también que en las pruebas de comunicación de voz no se garantizo la calidad de servicio ya que los objetivos principales de la tesis era probar que el sistema realmente funcionaba como se pensaba y ver las capacidades que tenían los routers para su correcto funcionamiento con el sistema planteado en el capitulo II.

5.2 Pruebas y resultados en el router Linksys WRT54G

Una de las pruebas que se le hicieron a cada router fue la prueba de conectividad, la cual consiste en enviar un paquete de prueba PING a su dirección configurada, que para el caso del linksys fue la 192.168.1.1, desde el computador en que se esta trabajando (con IP 12.168.1.3), si este paquete responde significa que el router se encontraba funcionando.

Para el caso de estos equipos, la prueba de conectividad se realizo para los dos protocolos de IP (Ipv4 e Ipv6) que se están utilizando. Para probar la conectividad en IPv4 se utilizo el comando "***PING 192.168.1.1***" lo que nos dio una respuesta positiva y esperada que se ilustra en a figura 5.1; ahora para el caso de la IPv6 se utilizo el comando pin6 2001:1310:a111:1211::1 y nos dio una respuesta satisfactoria que se puede ver en la figura 5.2.

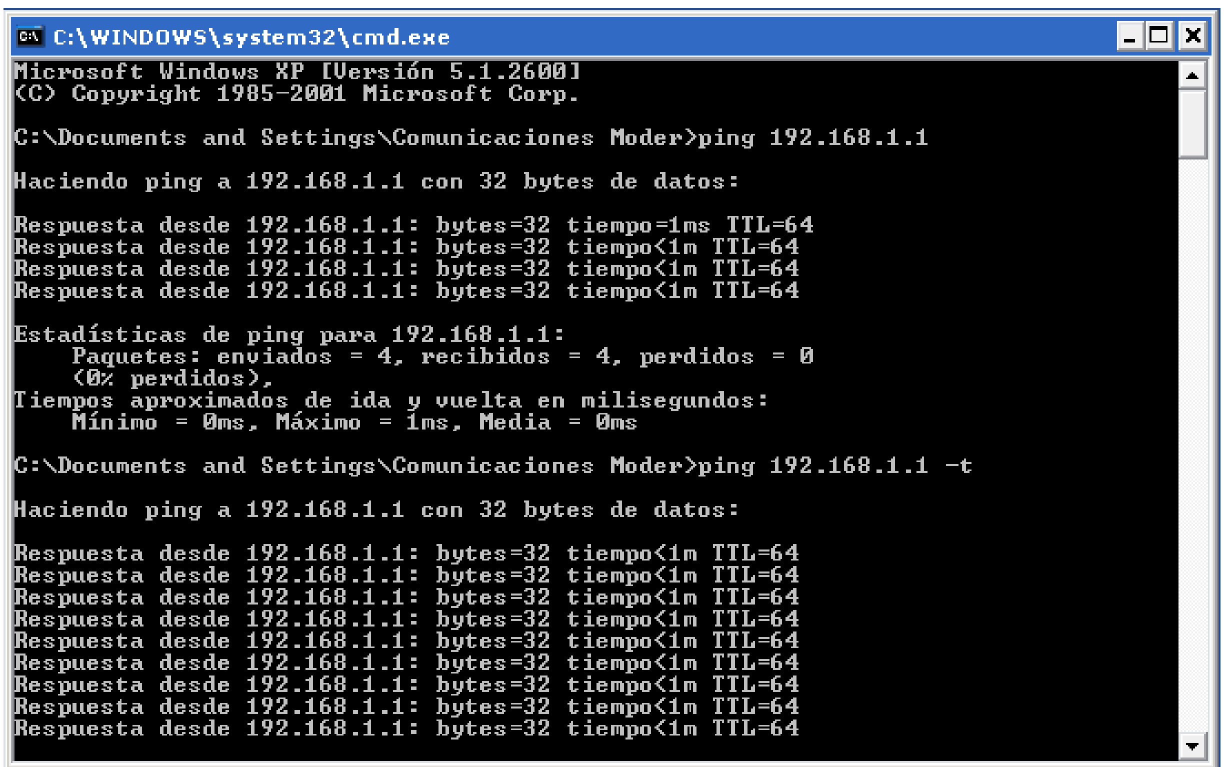


Figura 5.1 Repuesta del Ping IPv4

Importante es mencionar que el protocolo Ipv6 de los equipos solo funcionara si es activado el soporte para esta versión de IP que sale descrito en el capitulo IV.

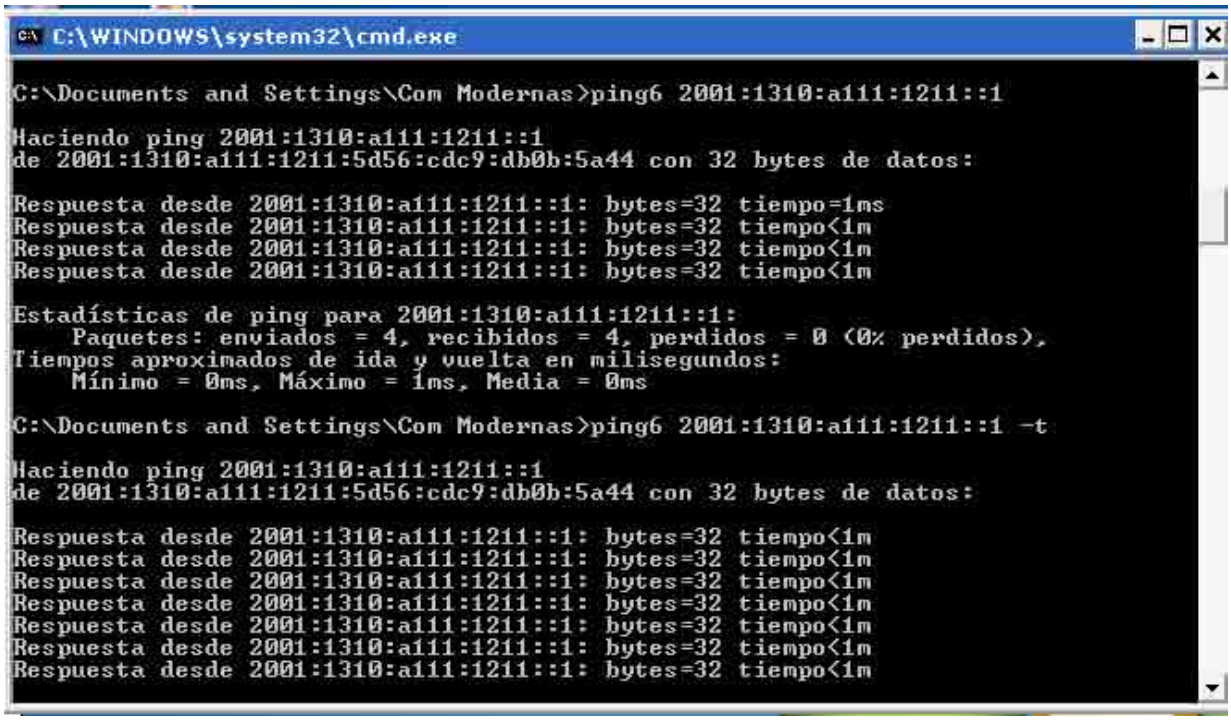


Figura 5.2: Respuesta del pin6

5.2.1 Prueba en IPv4

Luego de esto se procedió a realizar una llamada desde un PC con Ipv4 hacia otro PC con Ipv4 que estén dentro de la misma red, o sea conectados en el swicht del router, uno es el equipo cuya IP es 192.168.1.5 y el otro la IP 192.168.1.3 como muestra la figura 5.3.

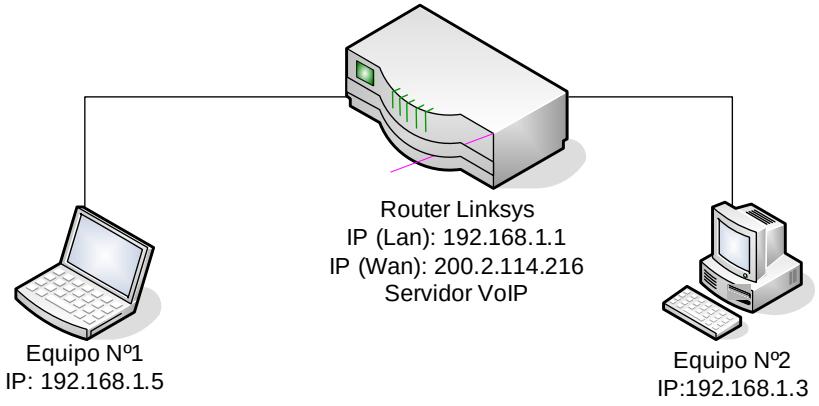


Figura 5.3: Primera prueba al router Linksys

Recordemos que el softphone que se utilizo en cada equipo fue el eyebeam, que se describe su configuración en el capitulo III. Con estos equipos se realizaron las llamadas y para ver el trafico de los paquetes que se estaban utilizando se utilizo el software Wireshark, el cual nos permitía ver los paquetes que se están traficando en la red que se estaba utilizando. En la figura 5.4 podemos observar el software eyebeam realizando una llamada del usuario 1 hacia usuario 2.

Figura 5.4: Llamada de VoIP en IPv4

Para comprobar que estábamos trabajando con la versión IPv4 de IP, se realizaron las mediciones que nos indicaban que se estaba trabajando con esta versión de IP, las cuales se pueden observar en la figura 5.5

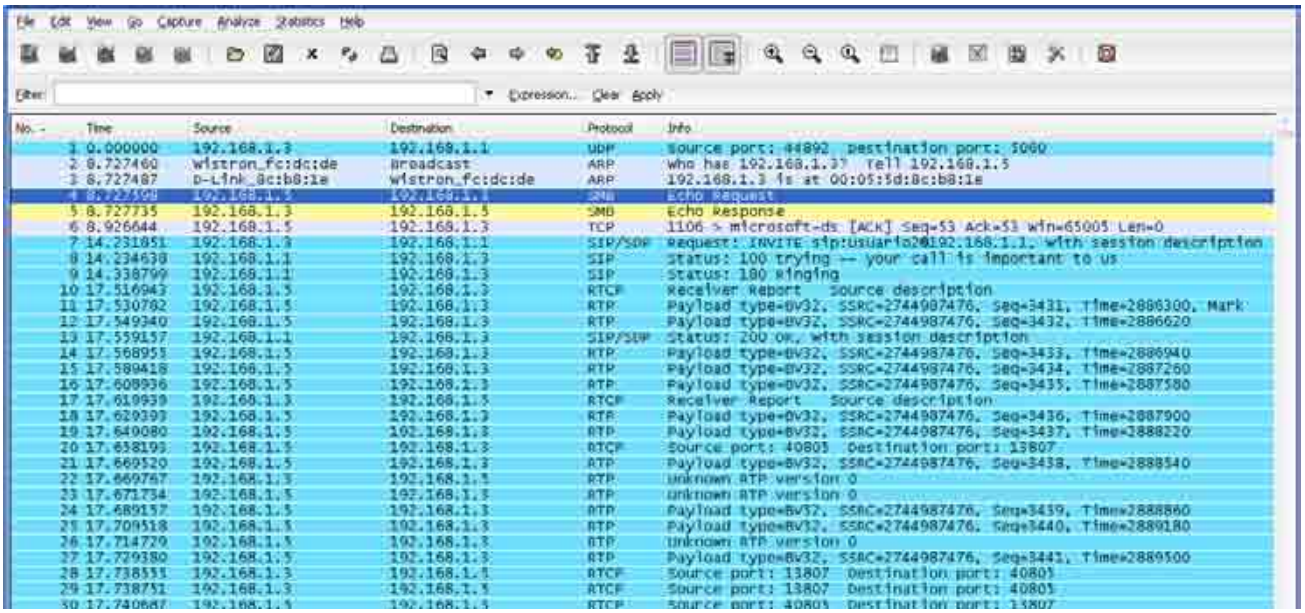


Figura 5.5: Paquetes IPv4 monitoreados

En la figura 5.5 se puede apreciar claramente los paquetes RTP que se están traficando y también que se esta utilizando el protocolo SIP para establecer la llamada entre los dos usuarios, tal como se esperaba, las respuestas al sistema han sido satisfactorias. Si observamos, también podemos apreciar los equipos en que se esta traficando la información, o sea las direcciones IP que tiene cada uno de ellos, ahora si se presentara otro equipo tratando de gestionar llamadas, también podría sin ninguna perdida en la calidad de la llamada. Ahora si se piensa en una cantidad superior de equipos, se debe tener en cuenta que el trafico a que se esta sometiendo al router es mayor por lo tanto la calidad de la llamada se puede ver afectada. Lo que va directamente relacionado con la cantidad de memoria de trabajo que posea el router, para el caso del router linksys la memoria es menor que la del router netgear, aunque existe la posibilidad de aumentar la memoria del linksys sin ningún problema.

También el openser posee una forma de identificar a los usuarios que se encuentran conectados a él y saber con que IP se encuentran conectados, además de entregar información adicional como es el numero y nombre de usuario, el softphone que se esta utilizando entre otras cosas que son de bastante utilidad para saber la cantidad de usuarios y la información de cada uno

de ellos. La figura 5.6 nos muestra esta opción que se puede desprender del comando ***"openserctl alias show"*** .

Figura 5.6: Monitoreo de usuarios del openser

Es importante destacar que se esta utilizando el modo por defecto del openser, es por esto que el dominio es por defecto y no nos muestra una información mas precisa, pero si se requiriera de varios dominios este método nos permitirá ver en que dominio se encuentra cada usurario, es por esto que resulta un método bastante bueno a la hora de tener información de los usuarios conectados al opeser.

5.2.2 Prueba con IPv4 e IPv6

Todo lo anteriormente descrito fue lo realizado para el trabajo pensando en dos equipos con la misma versión de protocolo, ahora si se desea comunicar dos equipos con distinta versión de protocolo, como lo es comunicar un equipo con protocolo Ipv4 con otro con IPv6, el procedimiento es similar, pero se debe tener en cuenta que el Openser debe estar corriendo con soporte para protocolo IPv6 y que el router tenga el soporte Ipv6 activado, por eso se le hace una prueba de conectividad Ipv6 primero como lo muestra la figura 5.2. El esquema montado para la prueba de comunicación IPv4 a IPv6 se muestra en la figura 5.7.

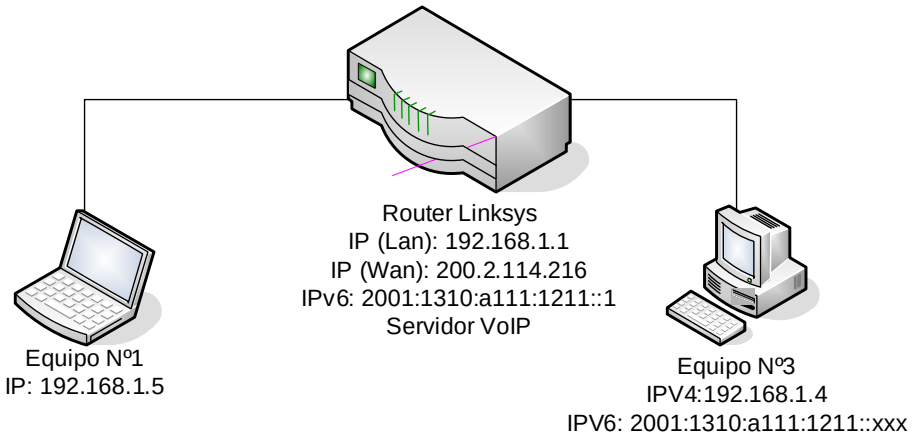


Figura 5.7: Comunicación IPv4 a IPv6

Tenemos que recordar que la dirección IPv6 es asignada a través de DHSP, es por esto que no se conoce la dirección del equipo por el momento.

Una ves echo esto, se procedió a realiza una llamada desde el equipo con IPv4 hacia el de IPv6 resultando la llamada exitosa, para luego realizar una llamada desde IPv6 hacia IPv4 también resultando exitosa.

Para comprobar que el openser si era capaz de soportar un sistema que trabajara con las dos versiones de IP, primero se comprobó los usuarios que se encontraban conectados con el comando "*openserctl alias show"* lo que arrojo como resultado lo que muestra la figura 5.8.

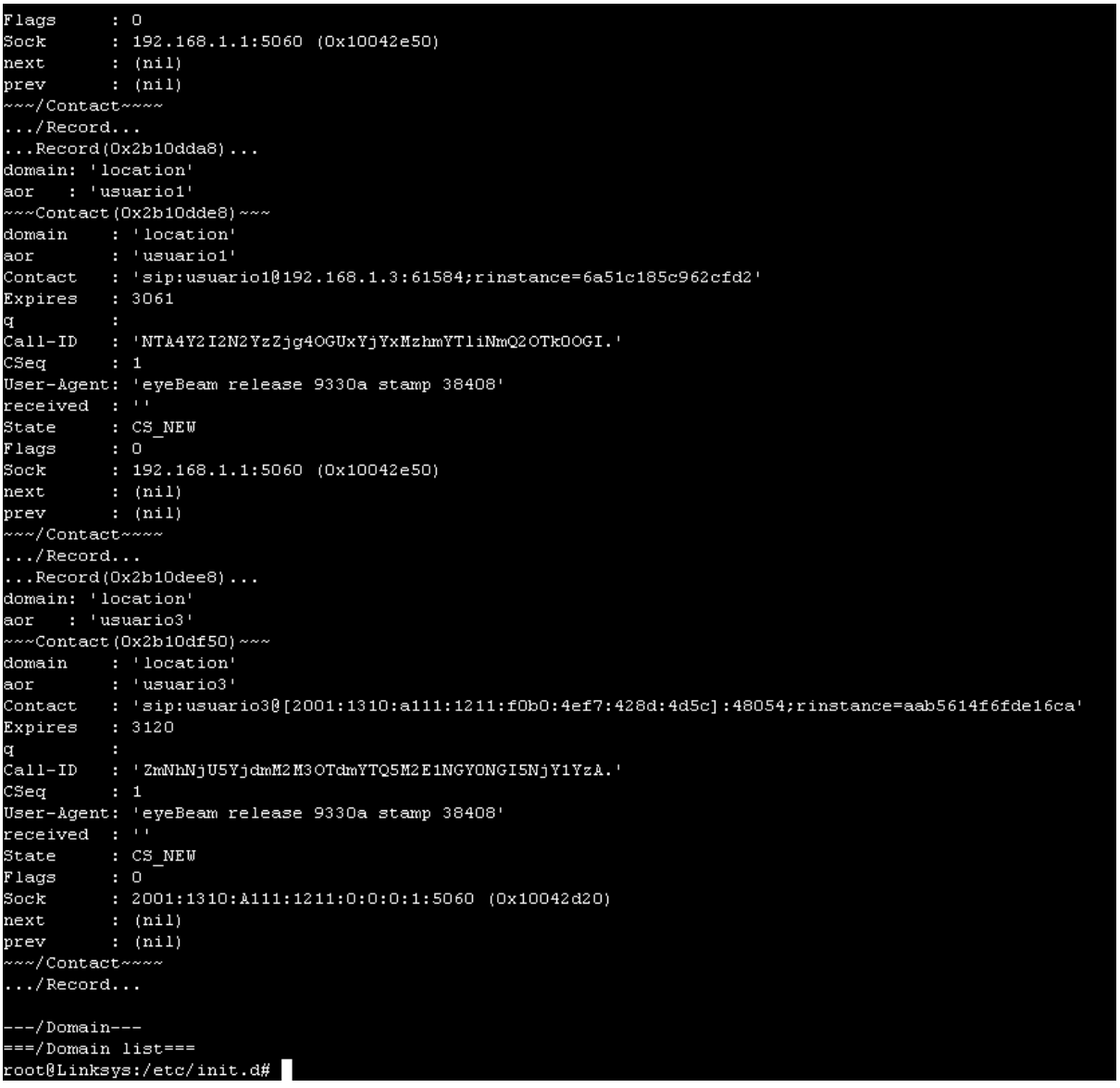


Figura 5.8: Usuarios openser con soporte IPv6

En la figura 5.8 se observa claramente los usuarios que están conectados y que versión de IP tienen, como el usuario 1 que esta con la ip 192.168.1.3 que es de IPv4 y el usuario 3 que es de IPv6 con la ip 2001:1310:a111:1211:f0b0:4ef7:428d:428d:4d5c. Así se pudo comprobar que el openser es totalmente compatible con las dos versiones de IP, el único cuidado es que hay que hacerlo partir de forma distinta a la tradicional, para que esto suceda hay que asignarle todas las ip que deseamos que escuche el sistema, es por lo que puede ser un poco complicado, pero las limitaciones de ip que se le asignen están dada por los usuarios de la re y la cantidad de servidores de voip que se necesite tener, aunque por lo general serán dos las ip que se utilicen, la ipv4 y la ipv6.

Luego para ver el trafico de paquetes que se genera para comprobar que si se esta trabajando con el protocolo Ipv6 y saber hasta que punto se transmite con ipv6, se realizo una llamada capturando los paquetes que se traficaban a cada lado de los equipos. Para esto se utilizaron los usuarios1 y usuario3, indicando en las figuras 5.9 y 5.10 los resultados de cada uno. Es importante mencionar que el tráfico desde y hacia un Terminal IPv6, desde el punto de vista de la captura de paquetes, es lo mismo, es por esto que solo se realiza en un solo sentido para el análisis.

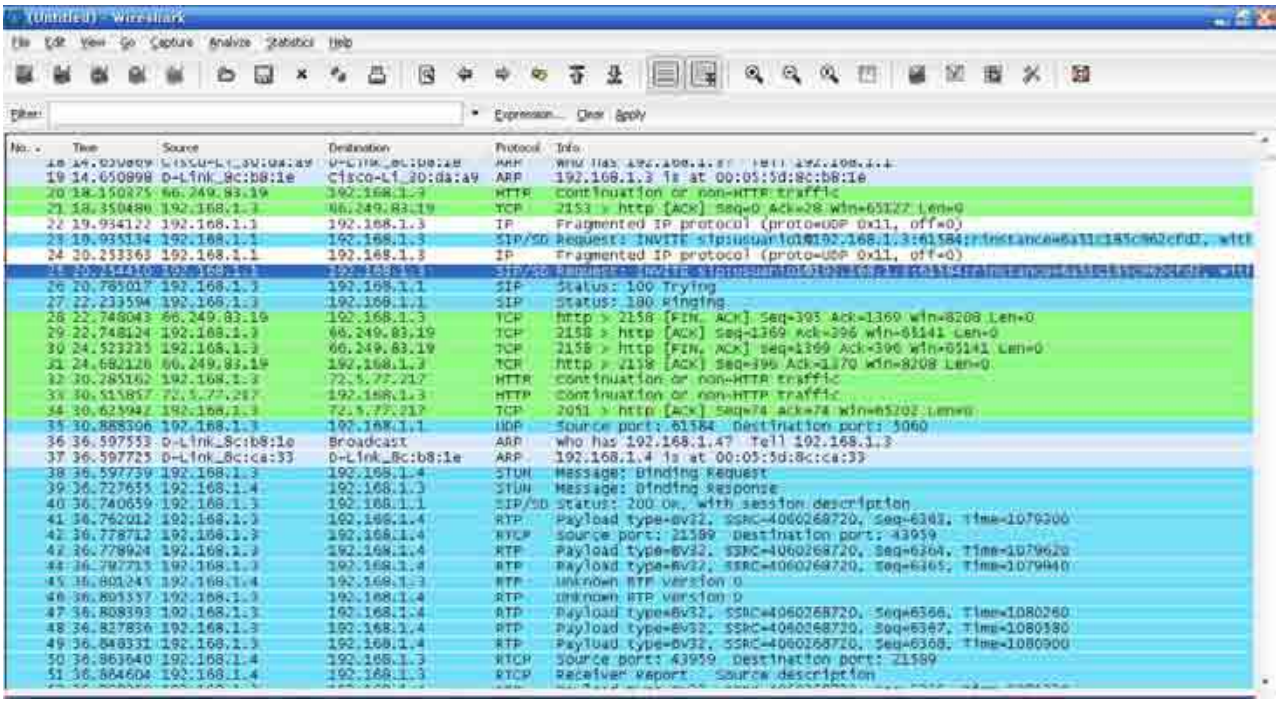


Figura 5.9: Llamada IPv4-IPv6 desde el equipo IPv4

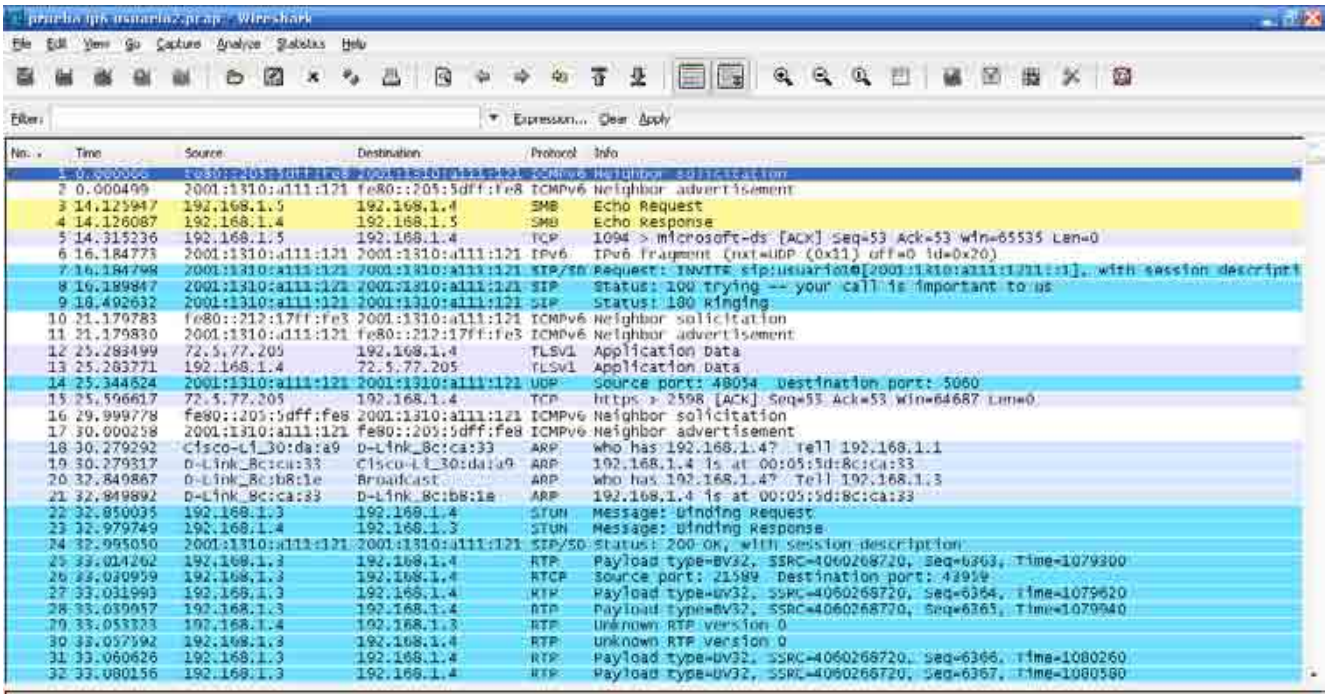


Figura 5.10: Llamada IPv4-IPv6 desde equipo IPv6

Podemos apreciar claramente en la figura 5.10 y la 5.9 que el trafico RTP se realiza en el protocolo IPv4, pero el protocolo SIP esta trabajando en IPv6 en el equipo que tiene el soporte para IPv6. Esto quiere decir que el protocolo de inicialización de sesión se encuentra gestionando bajo una dirección IPv6 y la voz que se transmite en los paquetes RTP sigue trabajando en IPv4 y utiliza la dirección IPv4 configurada en el equipo que se encuentra la dirección IPv6 y por lo tanto los paquetes de voz que llegan al otro extremos son ipv4 y se están escuchando bajo el misma versión de protocolo. Esto se debe a que el cliente SIP que se esta trabajando igual tiene soporte para IPv4, puesto que cuando se negocian los parámetros de la sesión media, los paquetes SDP contienen variaos codec RTP/IPv6, pero también se incluyen paquetes RTP/IPv4. Entonces cuando el segundo cliente esta trabajando en IPv4, entonces el programa trabajara con las direcciones nativas de IPv4 comunicándose así con IPv4, aunque el equipo que llama trabaja en IPv6. Esto se puede apreciar claramente en la figura 5.11, en donde los parámetros de sesión media tienen la opción de IPv4. Distinto es el caso cuando se trabaja con un sistema solamente basado en Ipv6, ya que hay si los paquetes RTP se trasmiten en Ipv6.

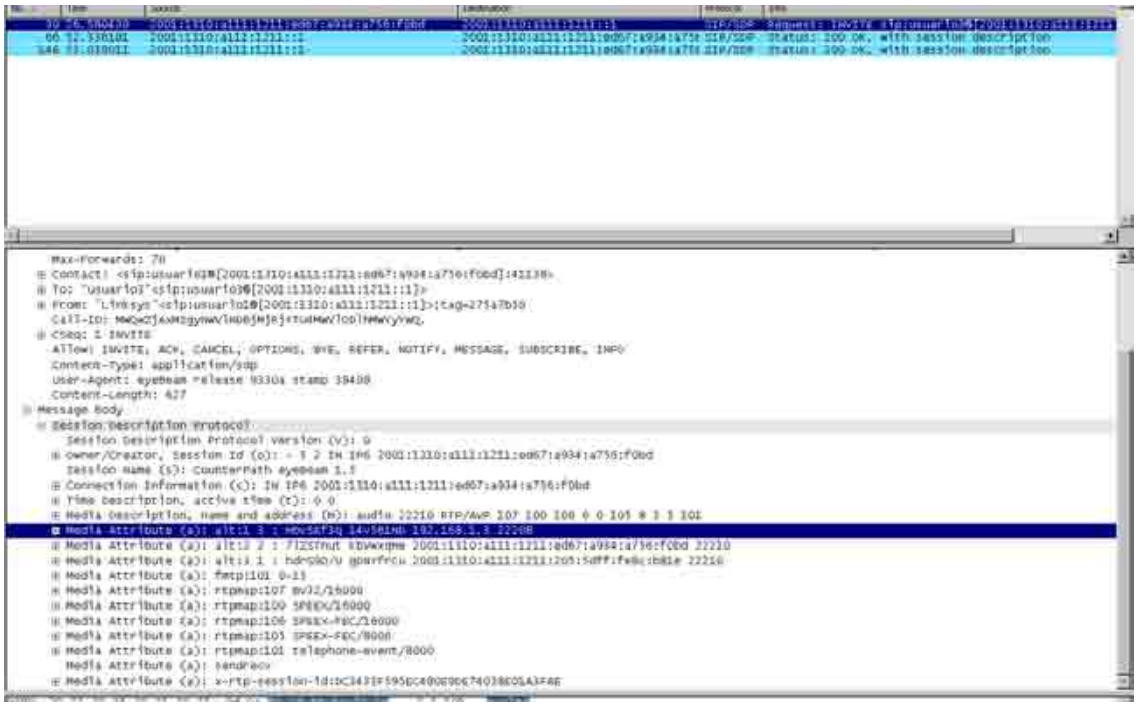


Figura 5.11: Parámetros del SIP/SDP

Ahora, en la figura 5.12, podemos apreciar que el protocolo SIP trabaja en ipv6 e ipv4, ya que la gestión de la llamada esta echa en IPv6

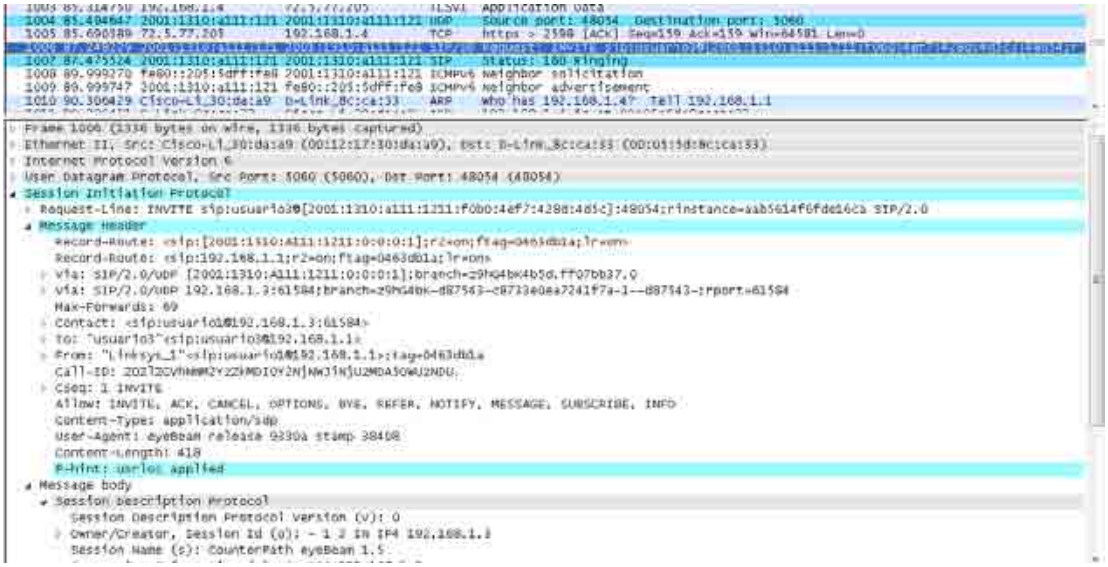


Figura 5.12: análisis del protocolo SIP en equipo IPv6

En la figura 5.12 observamos claramente la gestión que hace el protocolo SIP, en este caso el equipo que esta configurado con IPv4 esta llamando al equipo que esta con IPv6 y en esta figura podemos ver las versiones de IP que esta ocupando cada uno de los equipos en que están interviniendo en la llamada. En cambio en la figura 5.13 se ve que la llamada la esta realizando el equipo que tiene configurado el protocolo IPv6 hacia el equipo que tiene la versión ipv4, y podemos ver que los paquetes SIP que se están gestionando se encuentran en las dos versiones de IP en que se esta trabajando.

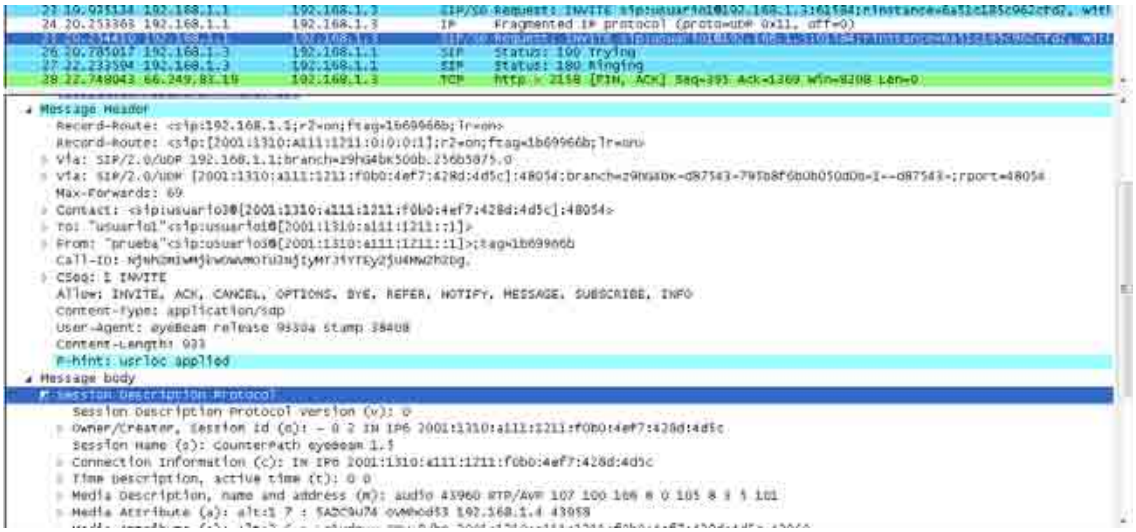


Figura 5.13: Análisis protocolo SIP en equipo IPv4

Según estos análisis la comunicación de VOIP entre los dos protocolos Internet se pude realizar sin ningún problema pero siempre teniendo en cuenta que los paquetes de voz que se transmiten siguen siendo en IPv4 ya que esta es la versión que se encuentra en común en los dos equipos.

5.2.3 Prueba con IPv6

A continuación la prueba que se realizo fue probar el equipo solamente trabajando con IPv6. Lo primero fue si el openser lograba reconocer los dos equipos en IPV6, lo que fue satisfactorio ya que se pudo sin ningún problema. En la figura 5.14 podemos observar los dos equipos que están reconocidos por el openser y con IPv6 los dos sin ningún problema.

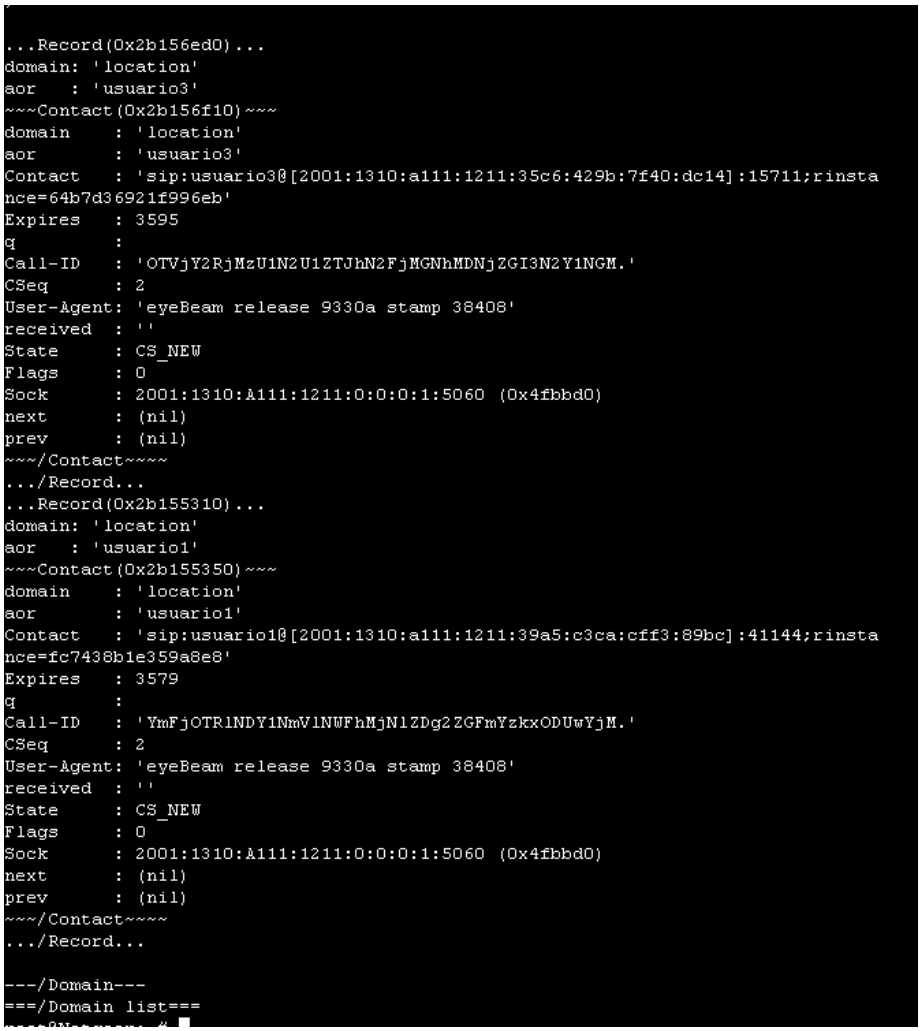


Figura 5.14: Equipos detectados en Ipv6 por OPenser

Ahora la figura 5.15 nos muestra el tráfico de paquetes realizado por una llamada desde IPv6 hacia IPv6, en donde los paquetes SIP y RTP lógicamente se transmiten en Ipv6 ya que estamos trabando solo con el protocolo IPv6 y en donde la calida de la llamada es levemente mejor ya que no hay tanto retardo y la calidad, desde el punto de la nitidez de la voz, es mejor que en el protocolo IPv4.

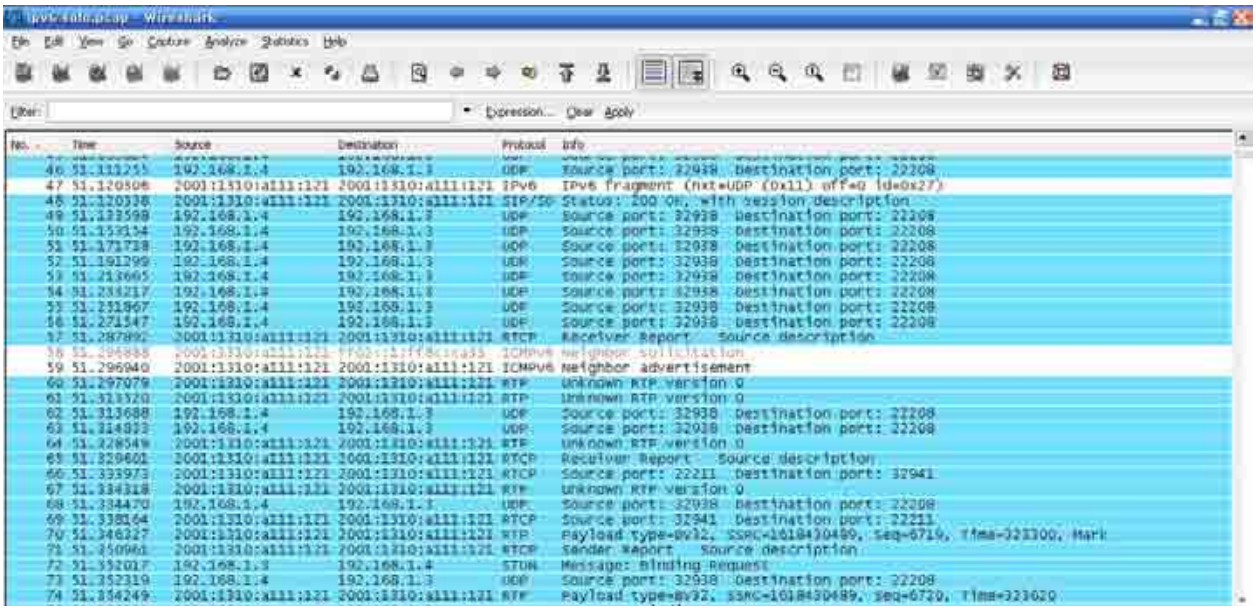


Figura 5.15: Trafico de paquetes en una llamada IPv6 – Ipv6

Bien con esta prueba finalizan las pruebas realizadas al router linksys y los resultados entregados se fueron describiendo a medida que se describían los procedimientos de prueba. Cabe mencionar que es sistema completo queda bastante limitado por las capacidades del router en que se este trabajando y la capacidad de la conexión Internet en que se este utilizando el sistema, ya que en un ancho de banda mayor se podría obtener una mejor calidad en la voz, aunque la calidad que se esta entregando en este sistema probado es bastante aceptable, aunque se ve una diferencia mínima, pero si diferencia en la calidad de la voz que entrega en IPv4 comparado con la calidad de voz que entrega un sistema puramente trabajando en IPv6, hay mucho menos ruido y eso hace que la voz se escuche mucho mas nítida que en el sistema basado en IPv4.

A continuación se presentan las pruebas realizadas al router netgear, aunque fueron las mismas que en el caso anterior así que no se detallaran demasiado, solo se pondrá énfasis en las diferencias que se pueda presentar.

5.3 Pruebas y resultados del router Netgear WGT634U

Las pruebas realizadas a este router son exactamente las mismas que para el router linksys, con la ventaja que en este router se contaba con mayor memoria de trabajo, por o tanto en este router era mucho mas fácil instalarle una mayor cantidad de programas y si se le suma las características especiales del frimware versión kamikaze que me permitía tener un monitoreo de la memoria y la velocidad de procesamiento de la cpu, entonces se volvía mucho mas fácil trabajar con este router. Pero las pruebas que se realizaron fueron las mismas, las cuales se detallan a continuación.

5.3.1 Prueba IPv4

La primea prueba fue comunicar un equipo en IPv4 con otro de IPv4 como muestra la figura 5.16.

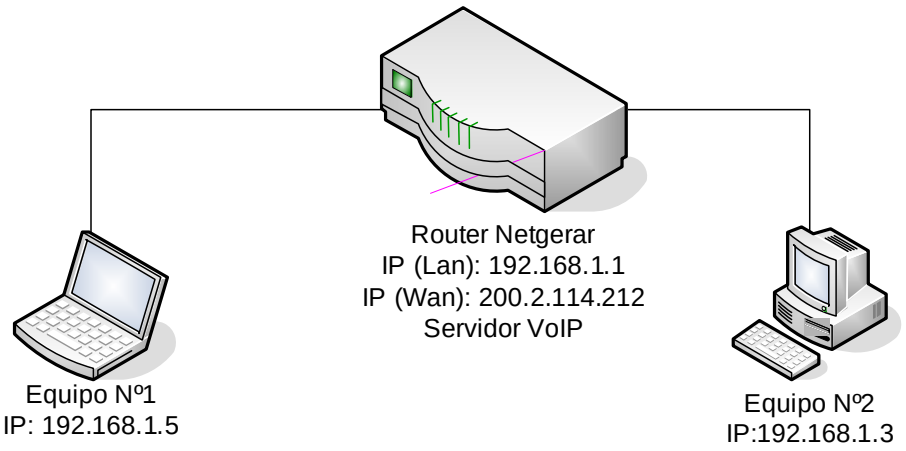


Figura 5.16: Comunicación en IPv4

Al igual que en el caso anterior, se utilizo el sofphone eyebeam para las comunicaciones y se realizó una llamada del equipo1 hacia el equipo 2, para comprobar la conectividad, resultando la llamada satisfactoria y de una mejor calidad que en el caso anterior, aunque como es habitual la calidad optima queda restringida a la cantidad de usuarios en la red.

La medición que se realizo con el Wireshark, se puede apreciar claramente en la figuras 5.17 y 5.18.

Figura 5.17: Paquetes Ipv4 Monitoreados 1

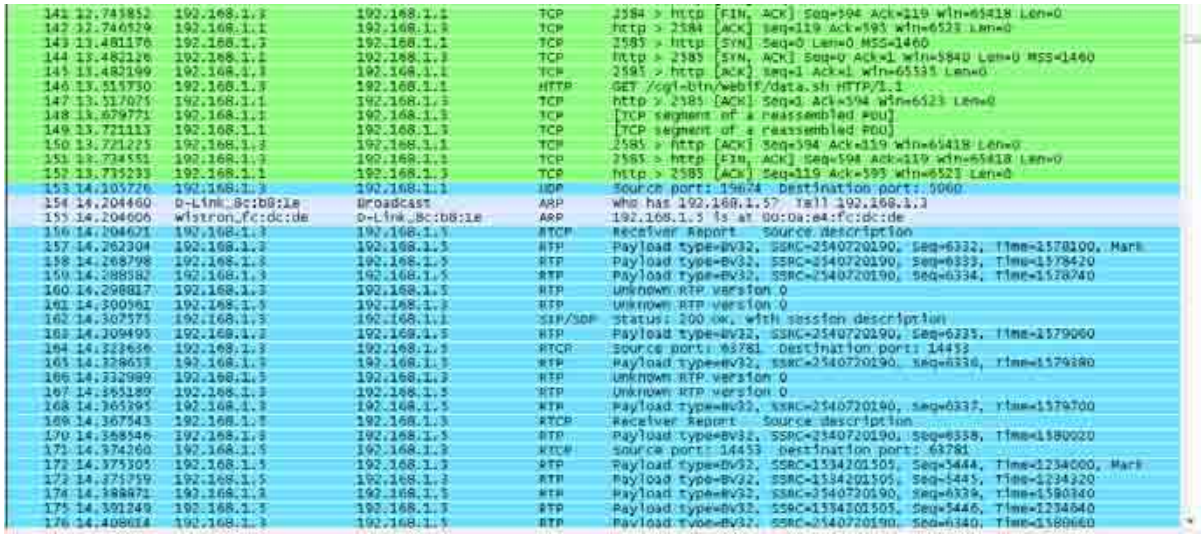


Figura 5.18: Paquetes Ipv4 Monitoreados 2

Como se observa, las diferencias desde el punto de vista del análisis de paquetes no es muy diferente a lo anterior, pero la diferencia esta en la velocidad de procesamiento de la información, con esto me refiero que el router linksys tenia una respuesta mucho mas rápida que el router netgear, a pesar que la memoria de trabajo del router netgear es mucho mayor comparado con la memoria del linksys. Esto se puede ver claramente en la cantidad de paquetes que se tarda en responder y en llegar los paquetes RTP a funcionar, a pesar que las pruebas fueron exactamente iguales además de las velocidades de repuesta, que en el linksys eran mucho mas rápidas que en el netgear.

La figura 5.19, nos muestra la herramienta de monitoreo de la puerta ethernet en donde esta conectado el usuario 2, ahí se puede apreciar claramente la taza de transferencia de datos que tiene el usuario y la cantidad de Kbps en que se transfiere la información, que en este caso es la voz que se esta transmitiendo a través del router. Es importante mencionar, que este tipo de medición no se tomo muy en cuenta ya que solo es de muestra que el frimware Kamikaze lo tiene y funciona, ya que no es un parámetro de comparación con el liksys por que el frimware del linksys no posee este tipo de información.

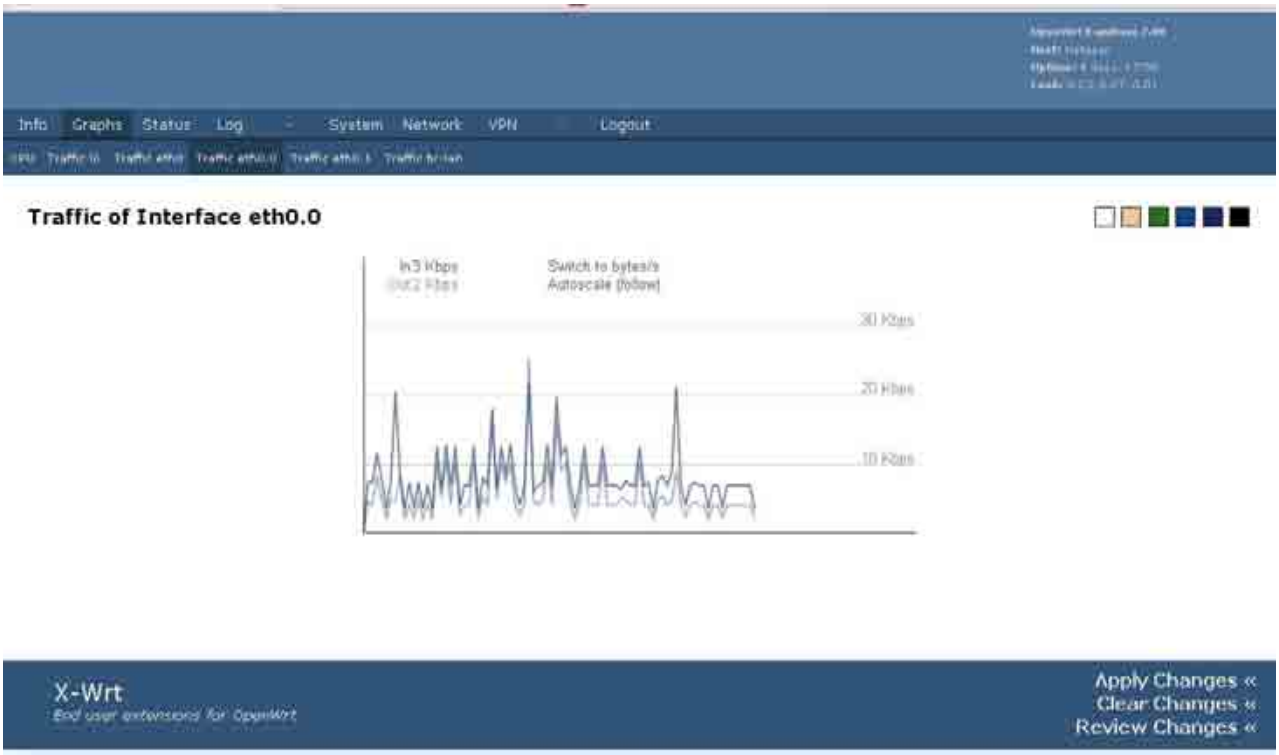


Figura 5.19: trafico del usuario 2.

Ahora en la figura 5.20, se pueden aprecias los usuarios conectados, como se ve esta conectado el usuario 1 y el usuario 2 con sus respectivas direcciones Ipv4. Con esto comprobamos que los usuarios están conectados al servidor de Voip y están listos para empezar a hacer llamadas entre ellos, como también podemos ver la información necesaria de cada usuario para saber cuantos clientes tenemos conectados en este momento.

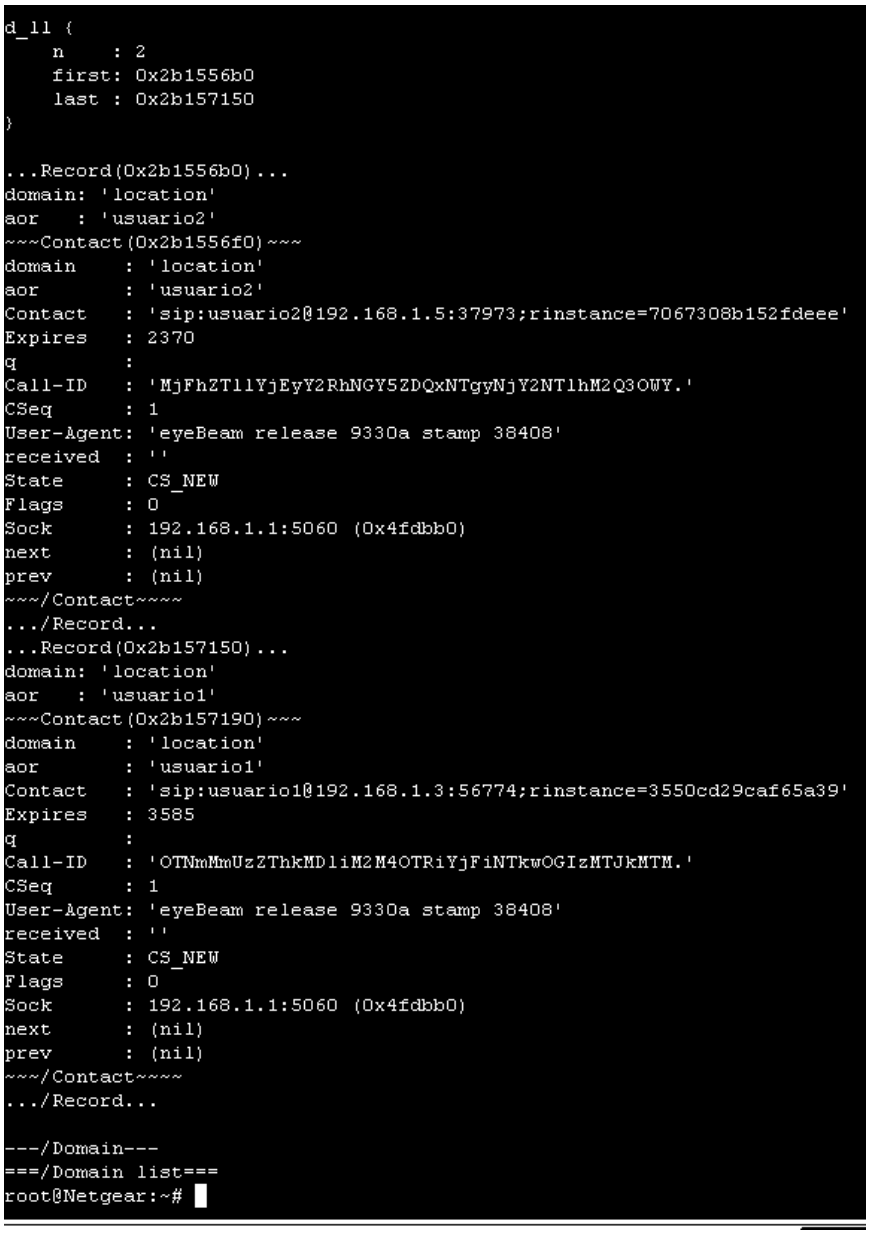


Figura 5.20: usuarios IPv4

5.3.2 Pruebas IPv4- Ipv6

Después de esto, e igual que para el linksys, se le realizaron las pruebas de comunicación en una red que contenga las dos versiones de IP (IPv4-IPv6). La figura 5.21 nos muestra el esquema e que se trabajo para estas pruebas.

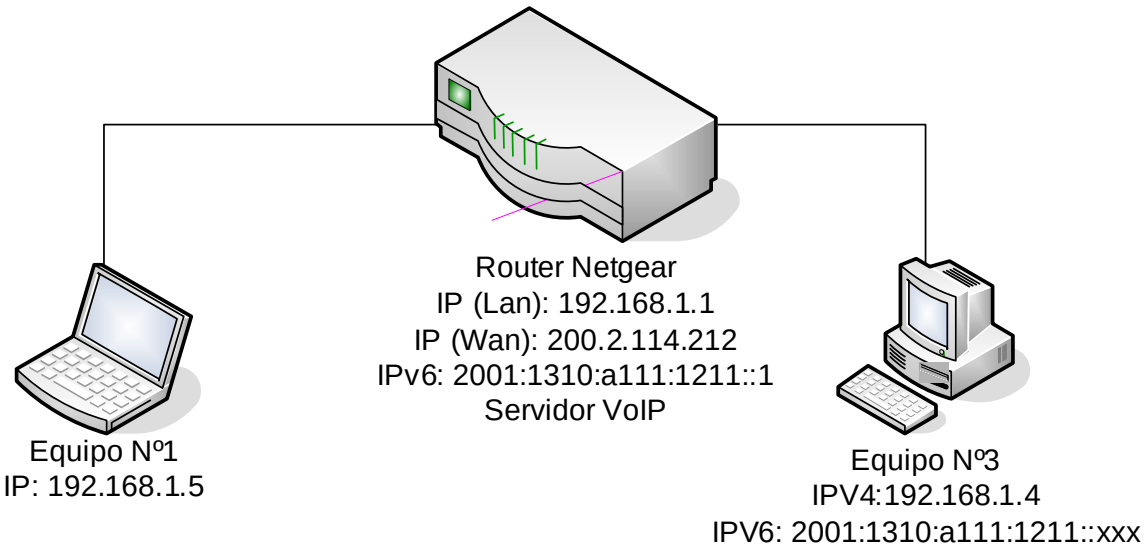


Figura 5.21: Pruebas IPv4- IPv6

Una vez mas utilizando el mismo softphone se realizo la comunicación en un equipo con IPv4 hacia otro con Ipv6, lo que al igual que en el caso anterior, resulto exitoso y sin mayores problemas, pero la velocidad de procesamiento de la información que contaba el router, igual se hizo notar en la calidad de la llamada, ya que presentaba cierto retardo y eso se refleja en el retardo del envío de los paquetes RTP hacia el destino.

Una ves más se observa que el equipo que cuenta con Ipv6 los paquetes RTP son enviados en IPv4, ya que es así como lo permite el protocolo SIP y además que como se cuenta con una IPv4 y Otra IPv6, entonces el Openser opta por la opción mas fácil y es enviar la voz a través de IPv4. Todo esto se observa en la figura 5.22 y 5.23, que muestra el tráfico de paquetes SIP y RTP de la llamada realiza.

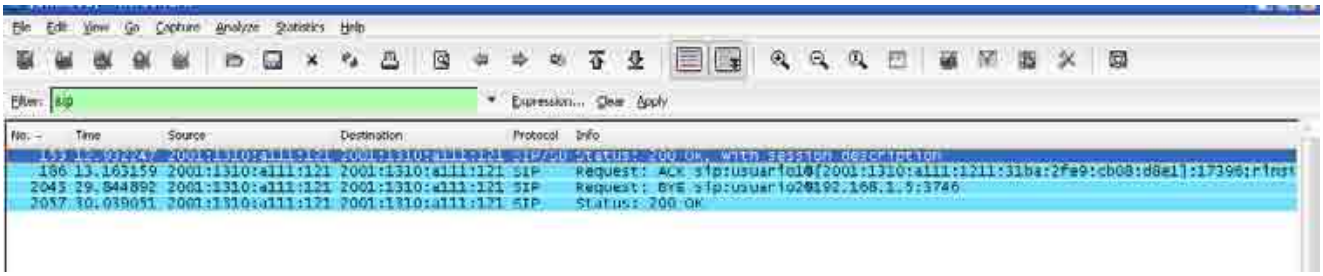


Figura 5.22: Tráfico de paquete SIP.

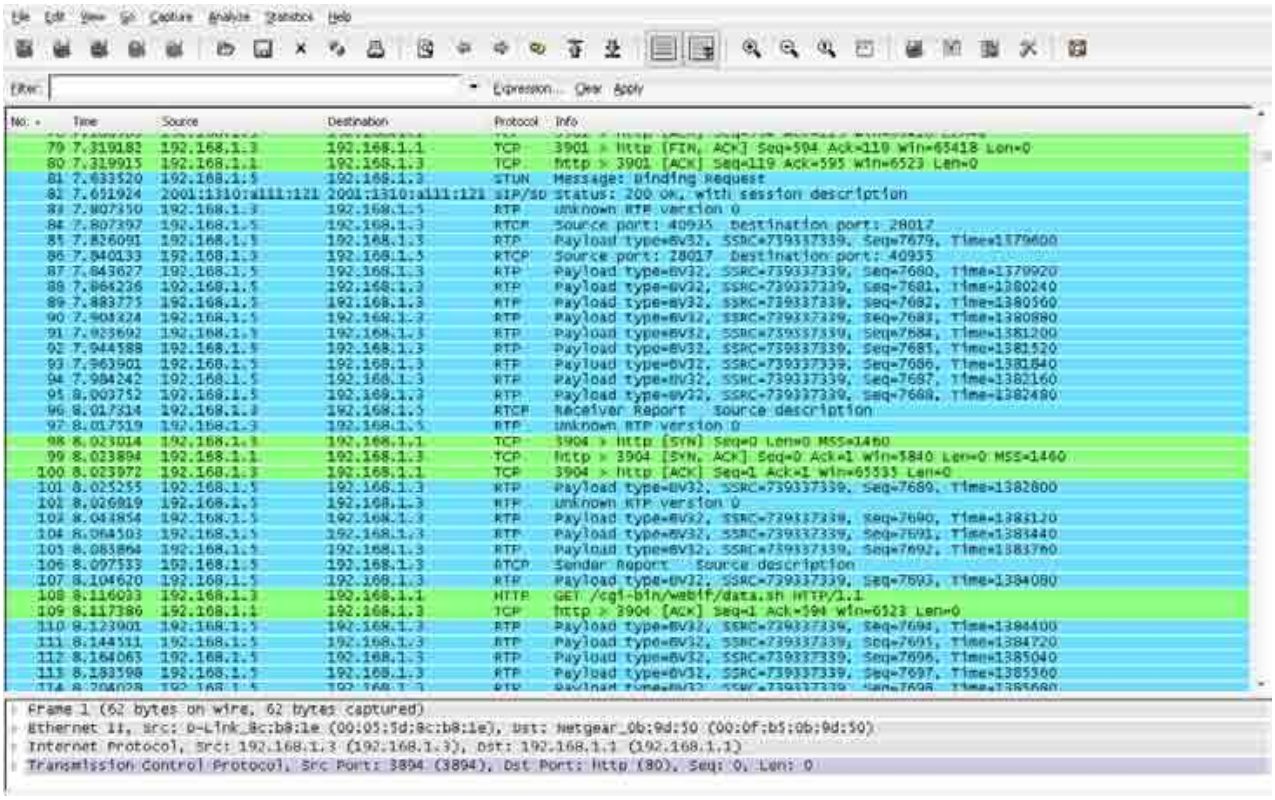


Figura 5.23: Tráfico de paquetes RTP

Bueno para este caso no hubo variantes que en la prueba con el linksys, ya que solamente influye la capacidad de procesamiento en la velocidad en que se transmiten los paquetes que se transmiten y obviamente en la calidad de la voz.

En la figura 5.24, nos muestra cuales son lo usuarios que se encuentran conectados al openser y a que versión de IP trabaja cada uno de ellos, como mucha información mas relevante que puede ser importante para futuras pruebas.

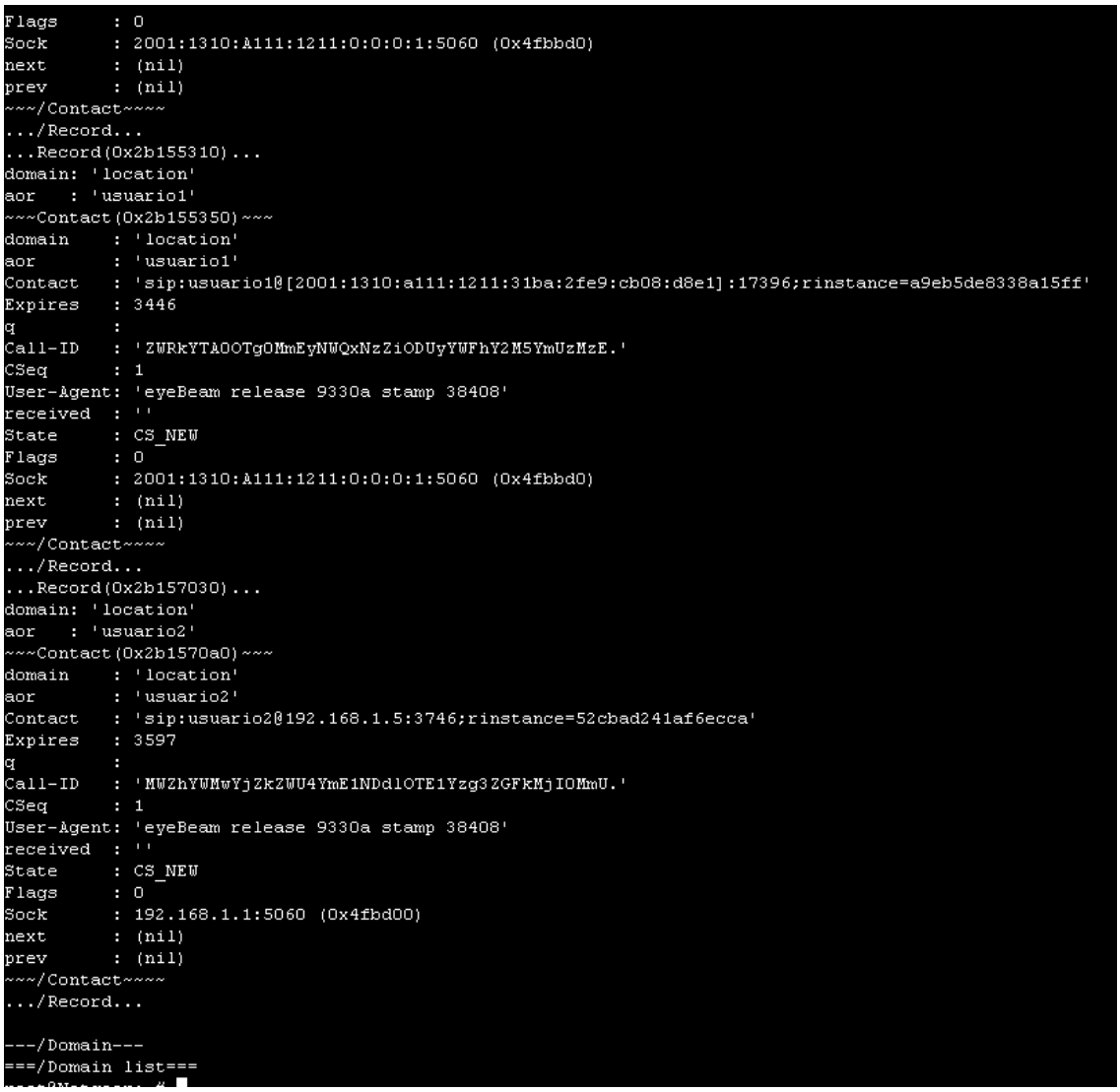


Figura 5.24: Usuarios conectados al openser

5.3.3 Pruebas Ipv6

Al igual que en los casos anteriores, se arranco el openser solo con soporte para IPv6 y se procedió a capturar los paquetes que se transmitieron y ver los usuarios si estaban realmente conectados con el protocolo IP deseado.

En la figura 5.25, apreciamos que los usuarios 1 y 3 se encuentran conectados correctamente con su dirección IP asignada por el router, sin ningún problema.

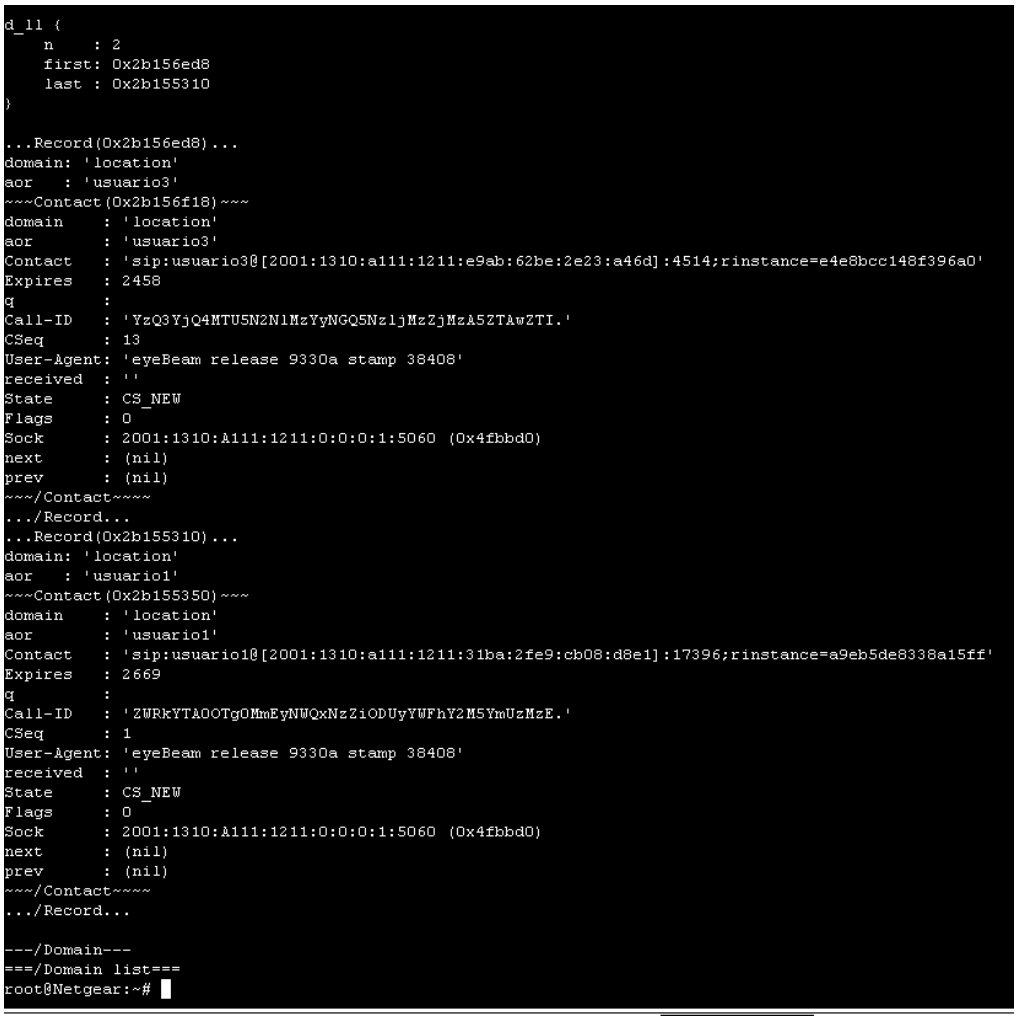


Figura 5.25: Usuarios conectados al openser

Luego, si observamos la figura 5.26 se puede apreciar el tráfico de paquetes SIP y RTP que se efectúan en una llamada que solo tiene IPv6. Como se esperaba los protocolos SIP y RTP se transmitieron en Ipv6 ya que era la única versión de IP que tenia configurada. Ya en la figura 5.27 observamos lo que esta asiendo el protocolo SIP, que es gestionar la llamada entre los usuarios que se desean con su respectivo protocolo involucrado, que para el caso es IPv6, aunque igual interviene el protocolo IPv4, pero como solo se esta utilizado IPv6, este no hace ningún efecto en la gestión de la llamada

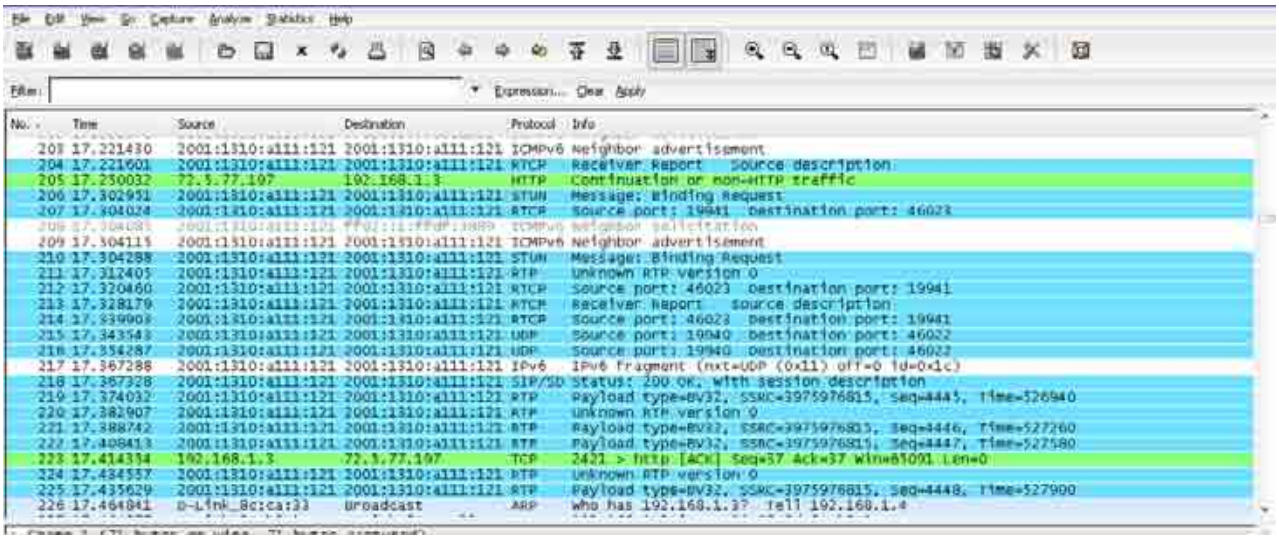


Figura 5.26: Trafico de paquetes IPV6

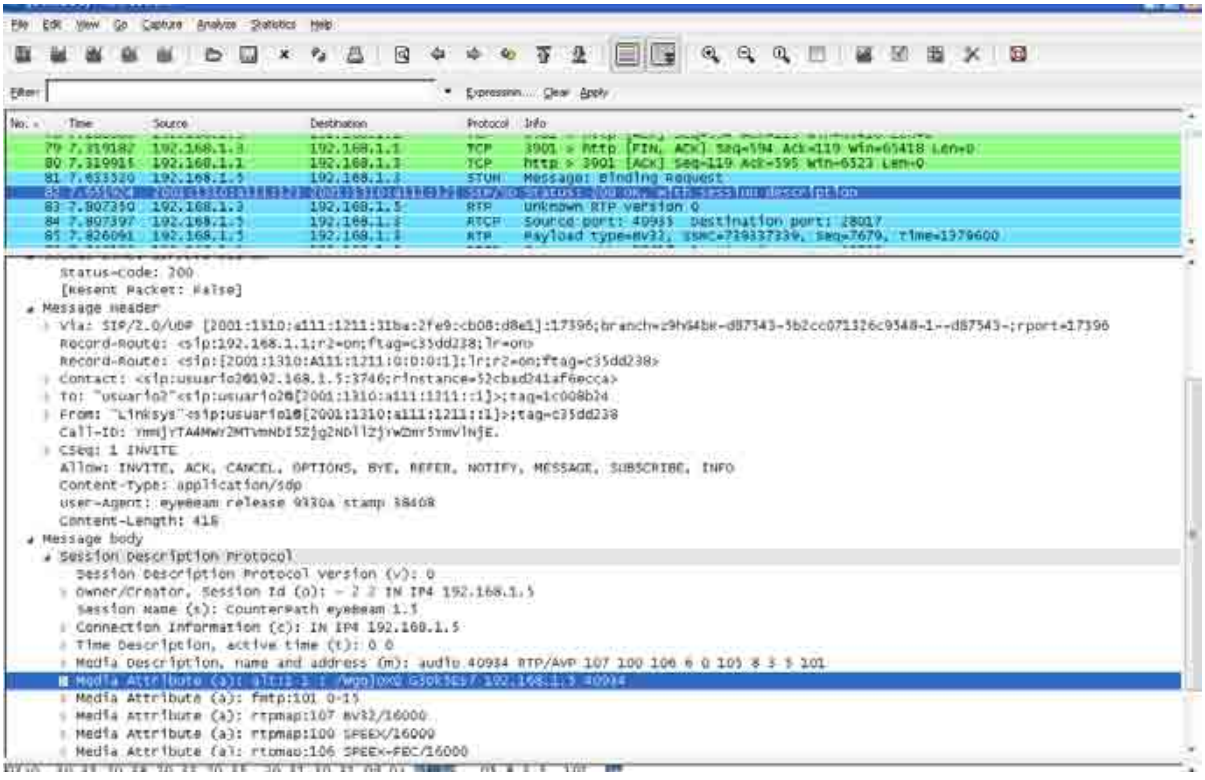


Figura 5.27: Análisis paquete SIP

Con esto han finalizado las pruebas que se le realizaron a los routers, y el análisis de las diferencias y principales observaciones se realizara a continuación.

5.4 Principales Observaciones, diferencias y propuestas de mejoras al sistema

Es importante comenzar a destacar que el sistema como se planteo funciona en perfectas condiciones, a pesar de las limitaciones de hardware, todo respondió de forma optima y sin mayores problemas, ya que el frimware y el openser trabajan súper bien instalados en estos software.

Ante las condiciones que se le plantearon todo respondió bien, y las diferencia que existieron entre uno y otro router, no fueron muchas ya que las condiciones eran casi idénticas; aunque si es importante destacar que el router netgear al tener menor velocidad de procesamiento de los datos, se volvía un poco tedioso esperar que cada comando se ejecute, pero las herramientas de monitoreo sirven de arto al momento de pensar en mas usuarios conectados, incluso si es que se llegase a necesitar soporte asterisk en el sistema, la versión kamikaze trae un soporte en Web sobre asterisk, lo que lo convierte en una situación bastante tentativa.

Una observación importante es que cuando se trabaja en u sistema con las dos versiones de IP, se convierte en un verdadero desafió el poder comunicar cada usuario en su dirección IP nativa. Esto se puede lograr instalando un recurso llamado mediaproxy y configurándolo con el openser para que trabaje en las dos versiones de IP, esto se podría lograr. Esto no se llevo a cabo ya que el objetivo era probar la funcionalidad del sistema, lo que puede ser interesante tocar en un futuro trabajo de titulación. La otra opción para cambiar esto, es que el softphone que se utilice en el usuario de IPv6, los codec de audio estén solo en IPv6, así se fuerza la openser trabajar solamente en esta versión de IP, resolviendo el problema planteado.

El otro desafió planteado para un siguiente trabajo de titulación, es configurar el sistema para que pueda pasar el firewall del router y el NAT, así pudiendo comunicar usuarios de dos redes LAN distintas. Para ello se puede utilizar el NATHELP que es una utilidad que trae para instalar el openwrt y así poder resolver en parte el problema que se plantea.

Algo importante igual de desarrollar es configurar la interfaz inalámbrica para probar el sistema con esta interfaz. En esta tesis no se realizo ya que solo nos interesaba la comunicación de dos usuarios pero en una interfaz alámbrica, siendo así realizada y finalizada con todas las observaciones ya antes realizadas.

Ante las pruebas relazadas es importante mencionar que el máximo de usuarios que se utilizaron fueron 4 lo que dejo por evidencia que todo funciona a la normalidad, ahora si el sistema se llegara a llevar al limite, el comportamiento de este es desconocido, aunque teóricamente las condiciones no deberían cambiar, excepto que sobrepase las capacidades del router o la red Internet que se este utilizando.

Con esto finaliza a investigación y el trabajo de titulación dejando abierta las puertas a nuevas aplicaciones o mejoras que se le deseen realizar al sistema implementado en el laboratorio de comunicaciones modernas del instituto de electricidad y electrónica.

CONCLUCIONES

Con el desarrollo de este proyecto de tesis ha quedado en evidencia que la utilización de un servidor en la telefonía IP no es indispensable, ya que con un router, que posea las características necesarias para la instalación de un frimware con código abierto como el Openwrt, se puede adaptar para el uso de servidor de Voip y de router a la vez, consiguiendo así la utilización al máximo de los recursos presentes en el router.

Es importante mencionar que la utilización del frimware openwrt en los router es bastante simple y de mucha ayuda para los equipos, ya que les explota los recursos al máximo y además tiene la opción de instalación de paquetes y manejo de su kernel para trabajar con las dos versiones de protocolos IP existentes, como lo es Ipv4 e Ipv6, además de poder transformar las maquinas en servidores de Voip, como muchas opciones mas que posee este frimware, sin contar que además se encuentra en desarrollo y cada vez mas usuarios están participando en la comunidad de Openwrt agregando nuevos avances mejorando así el frimware para nuevas utilizaciones.

Otro punto relevante en el trabajo de titulación, es que la cantidad de mejoras, paquetes y programas que se les desee hacer al sistema implementado va ha estar directamente relacionado con las capacidades que tenga el router a la ora de trabajar. Por ejemplo, cuando se le instalaron una cantidad determinada de programas al router linksys este dejo de funcionar correctamente ya que su memoria de trabajo estaba totalmente ocupada, distinto fue con el router netgear, que posee más memoria, se le instalo los mismo programas y éste si puedo seguir trabajando con normalidad, dejando en evidencia que es muy importante tener en cuenta las características de router al momento de realizar este sistema.

Al momento de hablar del programa openser, es importante el mencionar que este programa como PBX de paquetes SIP es bastante bueno, pero requiere de una gran cantidad de memoria para funcionar correctamente ya que en el router linksys que se utilizo, debía estar

funcionando solo, para que pueda correr de forma eficiente. También otro punto a considerar es el tipo de frimware que se desee instalar para poder utilizar el openser como PBX, ya que cuando se instalo el frimware kamikaze en el linksys, el openser no funcionaba, esto se debía a que la cantidad de memoria que le quedaba para trabajar era demasiado pequeña comparada con la que se requiere para el trabajo optimo del software.

La velocidad del procesador del router utilizado también es de vital importancia, ya que depende la velocidad en que se corran los procesos que se van a utilizar y en la eficiencia del sistema montado.

Al referirse al trabajo con los router, es importante tener en cuenta todas las variables al momento de instalar un frimware nuevo en ellos, ya que el mínimo error deja sin uso al router, y en algunos casos ni siquiera se pueden recuperar. Por ejemplo, al momento de instalar el frimware al un router linksys, como el que se utilizó, es relevante tener activado el boot_wait, que es este el que permite recuperar al router en caso de problemas y es el que acepta el frimware a través del FTP. Y para el caso del netgear, es tener un cable de consola adecuado par poder ingresar sin problemas a la bios del router y desde ahí actualizar los datos de sus puertas para así poder cargarle el frimware vía TFTP, aunque se recomienda siempre usar esta opción para el caso del trabajo con un router netgear.

Al trabajar con los dos tipos de protocolos, Ipv4 –Ipv6, se puede observar la diferencia que existe, desde el punto de vista calidad de voz. Aunque se puede decir que los parámetros de diferencia más importantes, para este sistema, son las capacidades de los router y la red en que se trabaje. Aunque en teoría, al momento de presentar más usuarios en la red, se podría producir una diferencia más notoria entre un protocolo y otro.

También al momento de trabajar con los dos tipos de protocolos (Ipv4-Ipv6), se pudo observar que la comunicación en un sistema que tenga las dos versiones de IP, los paquetes SIP se transmiten en el protocolo que tenga asignado cada usuario, pero siempre tiene un soporte para IPv4, entonces al momento de negociar los parámetros de la sesión de media, el SDP contiene varias opciones de codec sobre RTP/IPv6, pero también incluye una opción en Ipv4. Es por esto

que los paquetes RTP, para este caso, se transmiten en IPv4 nativa. Para solucionar esto, se puede configurar u mediaproxy adecuado, que funcione con openser y tenga soporte para IPv6, así se le asigna que los paquetes que tengan un SIP en IPv6 transmitan sus paquetes RTP en Ipv6; o también se pueden ajustar los codec del eyebeam para que el equipo con IPv6 trabaje solamente con esa versión de IP, negándole los codec para IPv4. Pero lo que nunca se puede hacer es eliminar la IPv4 del cliente windows, ya que es a través de esta que se puede crear la IPv6.

Y por ultimo, lo bueno de trabajar con un linksys o un netgear es que, para el caso del linksys, si bien su memoria de trabajo es limitada existen formas fáciles y seguras de expandírsela y así poder tener un router con mas capacidad de memoria Y para el caso del netgear, el puerto USB que posee nos permite almacenar mucha mas información, como por ejemplo una base de datos MSQL para los usuarios que pueda tener el sistema, haciendo lo así una opción bastante tentativa, ya que es en ésta base de datos en donde se guarda toda la información de los usuarios que utilizan este sistema, que para el caso del trabajo de titulación no se utilizo.

REFERENCIA BIBLIOGRAFICA

[1]. Andrew Tanenbaum , Redes de computadoras, 3ª edición, Ed. Prentice Hall Hispanoamericana, S.A, México, 1997

[2]. Rafael Conesa Pastor, José ManuelHuidobro Moya, Sistemas de telefonía, 5ª edición, Ed.Thomsom 2006

[3]. OpenWRT, http://wiki.openwrt.org/

[4]. Open WRT Wireless Freedom, http://openwrt.org/

[5]. Linux IPv6 HOWTO, http://tldp.org/HOWTO/Linux+IPv6-HOWTO/index.html

[6]. VoIP Foro, http://www.voipforo.com/ser/ser_introduccion.php

[7]. Sip Express Router, http://voip.megawan.com.ar/doku.php/sip_express_router

[8]. IPv6 Howto, http://wiki.openwrt.org/IPv6_howto

ANEXO 1: Herramientas de monitoreo del Frimware al Router

El router netgear, con la versión kamikaze instalada posee herramientas de monitoreo que ayudan a ver como se encuentra el estado del router, lo que lo hace un mucho mejor frimware que las versiones anteriores. En la figura 1 se puede ver un grafico del uso de la CPU.

Figura A.1: Utilización de la CPU

También posee gráficos de trafico de cada una de las puertas que posee, en las figura 2 muestra el trafico de la puerta eth0 y en la figura 3 la puerta LAN.

Figura A.2: Grafica Puerta eth0

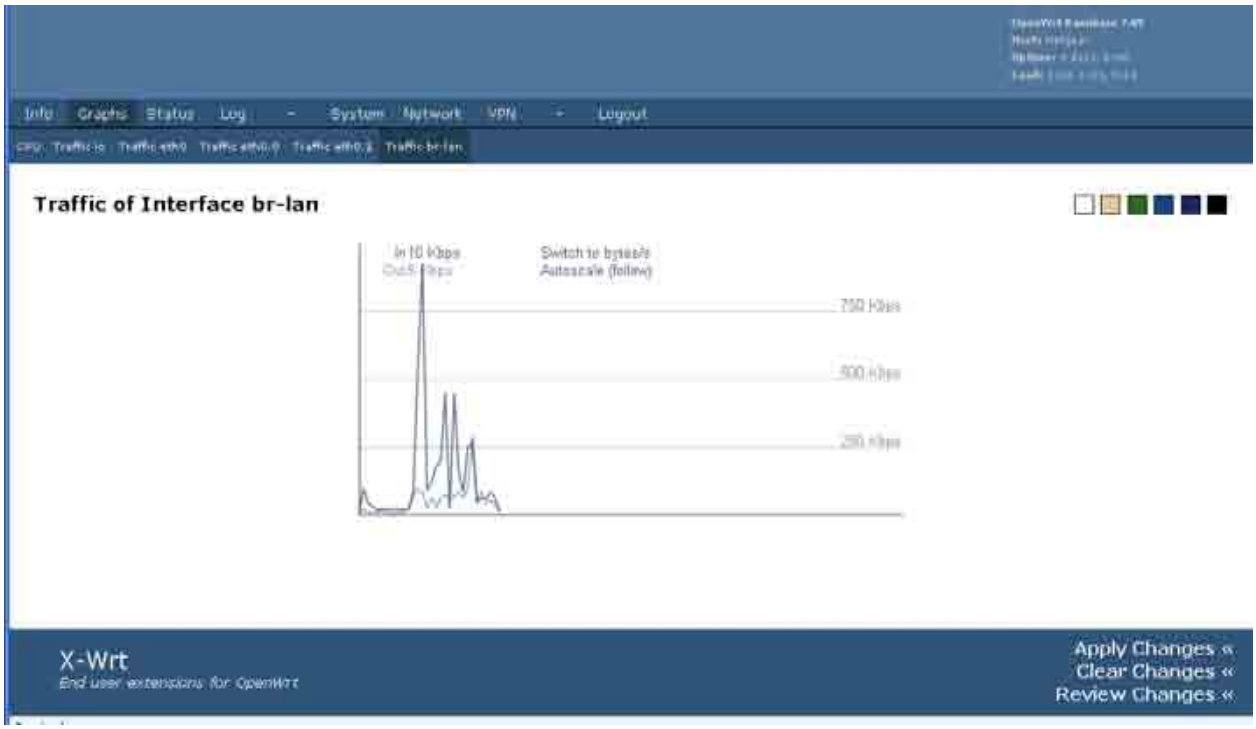


Figura A.3: Grafica Puerta LAN

También posee una pantalla que muestra la cantidad de memoria que utiliza y esta utilizando el router, lo que nos permite saber la cantidad de recursos que esta ocupando en un momento indicado. Esto igual se puede hacer en el otro router con la versión anterior, pero solo es a través de comandos y de una forma más complicada. La figura 4 muestra esta opción.

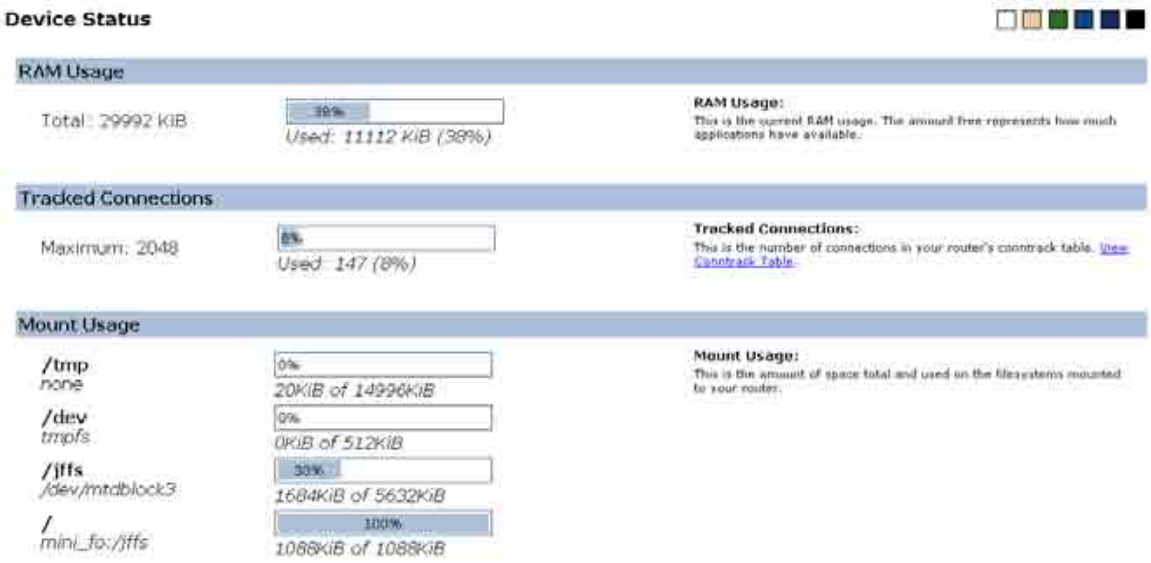


Figura A.4: Memoria utilizada

Cuenta con una lista de procesos que se muestra en la figura 5 y una serie de herramientas mas que posibilitan el monitoreo de los distintos procesos y recursos que se están utilizan en el router.

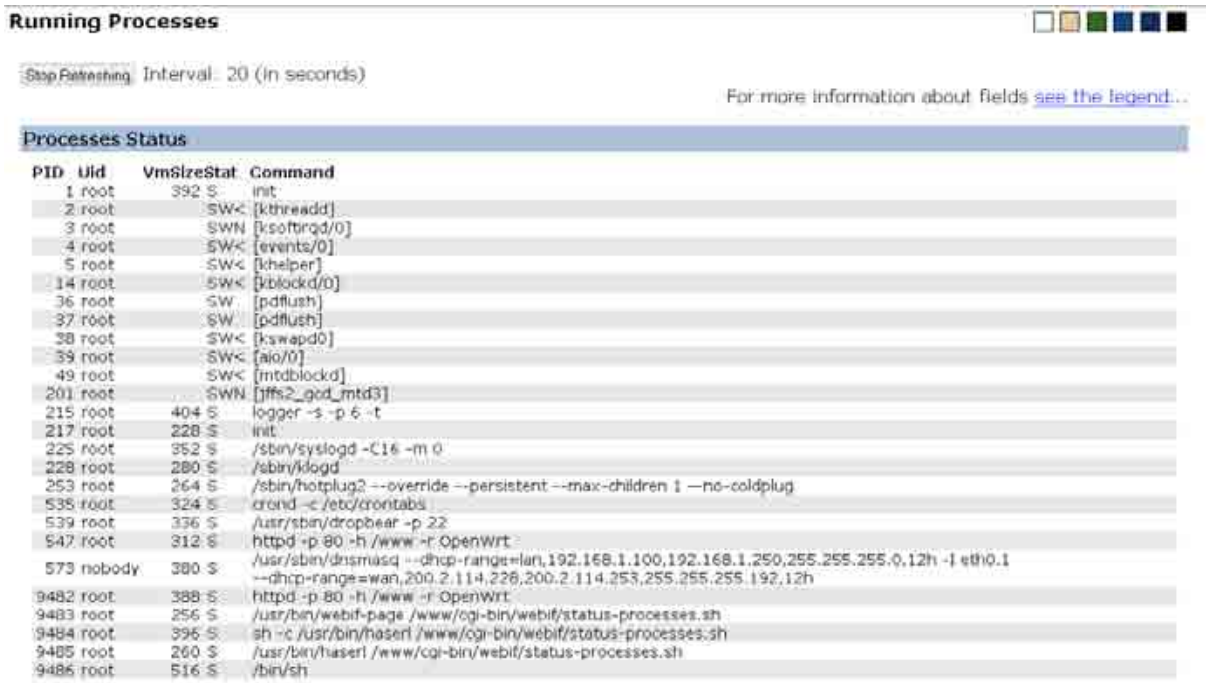


Figura A.5: lista de procesos.

Y así esta versión de frimware trae varias herramientas que se pueden utilizar para el monitoreo del router y as poder determinar cualquier problema que se presente o como también ver los recursos que quedan o que están utilizando los programas que se desea utilizar.

ANEXO 2: GLOSARIO DE TERMINOS

Lista de términos más importantes utilizados en el desarrollo de la tesis:

- ***VoIP (Voz sobre IP)***

  Tecnología que permite realizar llamadas dentro de la red TCP/IP

- ***ATM***

  Modo de transferencia asíncrona. El estándar internacional para relay de celdas en las que múltiples tipos de servicio (como, por ejemplo, voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de celdas se lleve a cabo en el hardware, disminuyendo por lo tanto los retardos en el tránsito. ATM está diseñada para sacar provecho de los medios de transmisión de alta velocidad como, por ejemplo, E3, SONET y T3.

- ***Banda ancha***

  Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica.

- ***Cisco Discovery Protocol***

  Protocolo de descubrimiento de dispositivos independiente de los medios y protocolos que se ejecuta en todos los equipos fabricados por Cisco, incluyendo routers, servidores de acceso, puentes y switches. Al usar CDP, el dispositivo puede advertir de su existencia a otros dispositivos y recibir información acerca de otros dispositivos en la misma LAN o en el lado remoto de una WAN. Se ejecuta en todos los medios que admitan SNAP, incluyendo las LAN, Frame Relay y ATM.

- ***CiscoWorks***

  Conjunto de aplicaciones de software para administración de internetwork basadas en SNMP. CiscoWorks incluye aplicaciones para monitorear el estado del router y del servidor de acceso, gestionar los archivos de configuración y diagnosticar los problemas de las redes. Las aplicaciones CiscoWorks se integran en varias plataformas de administración de red basadas en SNMP, incluyendo SunNet Manager, HP OpenView e IBM NetView.

- ***Host***

  Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

- ***Trama***

  Agrupación lógica de información que se envía como una unidad de capa de enlace de datos a través de un medio de transmisión. A menudo, se refiere al encabezado y a la información final, que se usan para la sincronización y el control de errores, que rodean a los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

- ***Softphone***

  Software que se utiliza para realzar llamadas a través de la red IP, desde un PC o equipo terminal.

- ***Full duplex***

  Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

- ***SIP (protocolo inicio de secion)***

  Nos permite negociar la llamada de VOIP dentro de una red IP

- ***TCP/IP***

  Protocolo Utilizado en Internet

- ***Script***

  Programa que se escribe para realizar actividades dentro de Linux.